Chaire L.R. Wilson
sur le droit des technologies
de l'information et du
commerce électronique

CENTRE DE
RECHERCHE EN
DROIT PUBLIC
Université de Montréal

Guide sur la mise en place et l'administration de mécanismes d'identification électroniques*

pour le
Secrétariat du Conseil du Trésor

Avril 2001

Pierre TRUDEL
Professeur
pierre.trudel@umontreal.ca

France ABRAN
Agente de recherche
france.abran@umontreal.ca

* Les auteurs tiennent à souligner l'apport de Bruno Georgescu et de Patricia Tourigny qui les ont assistés dans les recherches préparatoires à l'élaboration de ce document

SOMMAIRE

Une entreprise ou un organisme qui décide d'offrir ses services sur Internet doit prendre diverses précautions à l'égard de l'identification des personnes.

Ce guide vise à éclaircir la conduite à tenir dans la mise en place et l'administration de mécanismes d'identification électronique. Il accompagnera le développement de systèmes de transactions électroniques de manière à assurer le traitement adéquat de l'identité des personnes et des informations qui y sont afférentes.

On propose une démarche permettant de déterminer les risques reliés à l'identification dans un environnement de transactions électroniques de même qu'une méthode afin d'y implanter des mécanismes et processus adéquats d'identification.

La démarche est en quatre étapes.

Première étape : Spécifier les besoins d'identification

Dans un premier temps, on doit se demander si l'identification est nécessaire. L'identification peut s'avérer nécessaire en tant que composante d'une transaction. Par exemple, il est nécessaire de connaître l'adresse postale d'une personne pour faire la livraison d'un bien. Également, la loi exige souvent d'identifier un individu, par exemple, la loi sur le tabac interdit la vente des cigarettes aux moins de 18 ans. Finalement, une obligation d'identifier existe lorsque la transaction est telle que la prudence ou la bonne gestion impose que l'on identifie une partie.

Deuxième étape : Déterminer le degré de certitude requis pour l'identification

Compte tenu des enjeux et des risques des transactions qui seront réalisées dans l'environnement considéré, il s'agit ici de spécifier le degré de certitude dont on a besoin en matière d'identification. Par exemple, plus la transaction est importante, plus le niveau de fiabilité exigé sera élevé.

Troisième étape : Baliser la collecte et le traitement de l'information personnelle

Lorsque l'identification est nécessaire et après avoir déterminé le degré de certitude qui est requis, il faut considérer les limites imposées au nom de la protection de la vie privée des personnes. La loi empêche une entreprise ou un organisme d'exiger des renseignements personnels sur un individu qui ne sont pas nécessaires à la conclusion de la transaction ou à son exécution. Ainsi, selon la nature de la transaction ou des services à offrir, il faut limiter la collecte d'informations aux renseignements strictement nécessaires à la réalisation de cette transaction.

Quatrième étape : Déterminer les mécanismes et processus d'identification

Le choix de techniques et de mécanismes d'identification intervient en quatrième étape. Ces mécanismes et processus d'identification devront permettre d'identifier la personne avec un minimum d'informations personnelles et selon un niveau de fiabilité acceptable en conformité avec l'importance de la transaction.

Une fois l'identification effectuée, la loi prévoit des obligations quant à la collecte et le traitement des renseignements personnels. L'entreprise ou l'organisme doit informer l'individu du but de la collecte, de l'utilisation qui sera faite des renseignements, des catégories de personnes pouvant consulter son dossier, de l'endroit où il est détenu ainsi que de ses droits d'accès et de rectification à son dossier. De la même manière, l'entreprise qui détient, utilise ou communique les renseignements personnels ainsi obtenus doit en assurer la confidentialité. Elle doit voir à leur exactitude et à leur mise à jour au moment de les utiliser. Elle doit obtenir le consentement de l'usager lorsqu'elle désire les communiquer ou les utiliser à d'autres fins que celles déjà établies.

Table des matières

Introduction 1

L'objectif du guide 1
À quoi sert-il? 1
À qui est-il destiné? 1
Quelle est sa portée? 1
Quand doit-on s'en servir? 2

Identité, identification et processus d'identification 2
L'identité 2
L'identité légale 3
L'identification 3

La démarche proposée 5

1. Première étape : Spécifier les besoins d'identification 6

1.1 Pourquoi identifier? 7

1.2 Les situations où l'identification n'est pas nécessaire 7
1.2.1 Les situations où l'identification reste possible 8
1.2.2 Les situations où l'identification est habituellement impossible : l'anonymat 9

1.3 Les situations où l'identification est nécessaire 11
1.3.1 Les situations où une personne doit s'identifier 14
a) L'obligation explicite de s'identifier 14
b) Le devoir de s'identifier découlant des circonstances 14
1.3.2 Le devoir de s'assurer de l'identité d'une personne 15
a) Le devoir expressément prévu d'identifier 15
b) Le devoir d'identifier découlant de la nature de la transaction 17

2. Deuxième étape : Déterminer le degré de certitude requis pour l'identification 18

2.1 La démarche 19
2.1.1 Les enjeux de la transaction électronique 19
2.1.2 Les risques de la transaction électronique 20
2.1.3 Les exigences spécifiques à une transaction donnée 20

2.2 L'évaluation des risques et enjeux de la transaction 20
2.2.1 Enjeux modestes, risques faibles 22
2.2.2 Enjeux sensibles ou importants, risques moyens 23
a) L'identification sans le soutien de document 23
b) L'identification avec le soutien de documents 23
c) L'identification accompagnée de formalités 24
2.2.3 Enjeux très sensibles ou très importants, risques élevés 24
a) Les transactions nécessitant l'authenticité de l'information 26
b) Les transactions impliquant des informations confidentielles 27
2.2.4 Les risques et les responsabilités en matière d'identification 28

3. Troisième étape : Baliser la collecte et le traitement de l'information personnelle 31

3.1 La démarche 31

3.2 Les principes de gestion à respecter 33
3.2.1 La nécessité de la collecte d'informations identifiantes 33
3.2.2 La détention limitée dans le temps 34
3.2.3 La qualité des données 35

3.2.4 Les garanties de sécurité 35
3.2.5 La transparence 36
3.2.6 La responsabilité 37
3.2.7 La participation individuelle 37

3.3 Les devoirs et obligations relatifs au traitement et à l'utilisation de l'information identifiante 37
3.3.1 La démonstration de la nécessité de la cueillette 38
3.3.2 Le traitement 38
3.3.3 L'utilisation et la communication des renseignements personnels 39

4. Quatrième étape : Déterminer les mécanismes et processus d'identification 42

4.1 Les mécanismes et processus d'identification fondés sur l'information obtenue de l'usager 43
4.1.1 Les messages électroniques 43
4.1.2 L'usage du nom 43
4.1.3 Les formulaires 43

4.2 Les mécanismes et processus d'identification fondés sur ce que l'usager connaît 44
4.2.1 Le code secret 44
4.2.2 Le numéro d'identification 45

4.3 Les mécanismes et processus d'identification fondés sur ce que l'usager possède 45
4.3.1 Les jetons physiques 46
4.3.2 Les cartes à microprocesseur 46
4.3.3 La signature numérique 47

4.4 Les mécanismes et processus d'identification fondés sur ce que l'usager est - les données biométriques 48

4.5 L'identification par le recours à un tiers 50
4.5.1 La certification par un tiers 50
4.5.2 Les certificats 51

4.6 Les autres techniques d'identification sur Internet 53
4.6.1 Les fichiers témoin (*cookies*) 53
4.6.2 Les variables d'environnement 54
4.6.3 Le fichier d'audit du serveur 55
4.6.4 La mémoire cache 56

4.7 Les moyens indirects d'identification 57

5. L'attribution d'une identité dans les environnements électroniques 60

5.1 L'identité que la personne s'attribue elle-même 60
5.1.1 L'identification de l'adresse électronique 60
5.1.2 Les renseignements personnels fournis en ligne 60

5.2 L'identité attribuée par une personne 61
5.2.1 La vérification effectuée auprès de tiers de confiance 61
5.2.2 La vérification des pièces justificatives 61
5.2.3 La vérification d'identité par la présence physique des personnes 61

5.3 L'identité attestée 62

Conclusion - Récapitulatif sur la conduite à tenir en matière d'identification électronique 65

Annexe 1 - Tableaux 67
Annexe 2 - La signature numérique 75
Annexe 3 - Les techniques biométriques 80

Introduction

Il convient ici de préciser l'objectif du présent guide et de rappeler certaines notions générales liées à l'identité et à l'identification.

L'objectif du guide

L'identité concerne la reconnaissance d'une personne. Dans la vie sociale, cette reconnaissance est généralement basée sur des caractéristiques physiques et corporelles qui font que l'être humain existe comme être unique et ne se confond avec aucun autre. L'identification consiste à établir l'identité de quelqu'un, son état civil, pour pouvoir dire qui il est et nous permettre de le distinguer des autres.

Dans le contexte des transactions électroniques, l'identité concerne les informations et les processus procurant le degré requis de certitude au sujet de l'identité d'une personne. Dans un environnement comme Internet, ces informations s'obtiennent habituellement lors du déroulement des moindres interactions.

Le but de ce guide est d'éclaircir la conduite à tenir dans la mise en place et l'administration de mécanismes d'identification électronique. Il vise aussi à accompagner le développement de systèmes de transactions électroniques, afin d'assurer le traitement adéquat de l'identité des personnes et des informations qui y sont afférentes. On y expose une démarche permettant de déterminer les risques reliés à l'identification dans un environnement de transactions électroniques de même qu'une méthode afin d'y implanter des mécanismes et processus adéquats d'identification.

À quoi sert-il?

Ce guide explicite les préoccupations relatives à l'identité et à l'identification des personnes dans le cadre des environnements électroniques dans lesquels se réalisent des transactions. Il précise les exigences et les conduites à tenir dans le développement et l'exploitation de tels systèmes.

À qui est-il destiné?

Ce guide est destiné principalement aux personnes responsables de la mise en place et de la gestion de sites ou environnements électroniques dans lesquels se déroulent des transactions. Il pourra également fournir des informations utiles à tous ceux qui œuvrent à la conception, au développement et à l'implantation de systèmes d'information destinés à soutenir des échanges transactionnels.

Quelle est sa portée?

Bien que les questions relatives à l'identification des personnes se posent en une multitude de situations dans le monde virtuel ou ailleurs, le présent guide traite principalement des mécanismes d'identification dans le cadre des échanges prenant place dans des environnements électroniques de type Internet.

Quand doit-on s'en servir?

Ce guide devrait être utilisé dès la conception de sites ou de systèmes nécessitant l'identification des personnes. Il accompagnera également les gestionnaires ayant besoin d'informations plus précises sur les droits et obligations des citoyens et de l'Administration en matière d'identification.

Identité, identification et processus d'identification

Dans cette partie, sont présentées les notions fondamentales relatives à l'identité et à l'identification. On caractérise aussi le processus d'identification afin de situer où et comment se posent les exigences déontologiques et juridiques qui doivent être respectées.

L'identité

Par «identité», on entend «le fait, pour une personne, d'être un individu donné et de pouvoir être légalement reconnu pour tel sans nulle confusion grâce aux éléments (état civil, signalement) qui l'individualisent». L'identité est un concept difficile à cerner puisque son sens peut différer selon les domaines de la connaissance dans lesquels on se situe.

Comme il n'y a pas de critères de définition universels du concept, les contours de l'identité demeurent difficiles à circonscrire. L'identité d'une personne s'apprécie en effet selon la communauté relationnelle dans laquelle ses actions s'inscrivent. Toute personne appartient en effet à diverses communautés relationnelles qui l'identifient de façons différentes. Dans son quartier, une personne peut être identifiée que comme étant «le voisin qui habite la maison en briques rouges». Bien que rudimentaire, cette identité est suffisante aux besoins de la surveillance de quartier. Dans son milieu de travail, cette personne n'est peut-être connue par plusieurs collègues que par sa fonction ou son apparence physique. Ce sera, «la secrétaire de Marc» ou encore le «grand blond frisé avec des lunettes !» Encore ici, cette identité est suffisante eu égard aux besoins du milieu. Plus les relations interpersonnelles seront étroites ou considérées comme importantes ou à risques, plus l'identité d'une personne requiert de la précision. C'est ainsi que l'interaction de l'être humain avec ses semblables a imposé la mise en place d'un système consacrant la stabilité de l'identité des personnes.

Ensuite, l'identité est un concept qui prend également différents sens selon le champ de connaissance à partir duquel on l'aborde. La philosophie, la psychologie, les sciences sociales et les sciences pures en ont leurs propres définitions qui s'interprètent en fonction du champ étudié.

D'un point de vue juridique, l'identité concerne l'ensemble des données de fait et de droit qui permettent d'individualiser quelqu'un. Les identificateurs tels les pièces d'identité, les passeports, les permis de conduire etc., permettent d'établir les éléments qui, légalement, concourent à l'identification d'une personne physique dans la société au regard de l'état civil : nom, prénom, date de naissance, filiation etc. Au niveau judiciaire, établir l'identité consiste à assurer, par différents moyens techniques, l'identification de certaines personnes.

L'identité légale

À la naissance, chaque personne se voit attribuer un nom et un prénom qu'elle conserve toute sa vie et sous lesquels elle a l'obligation d'exercer ses droits civils (art. 5 et 50 C.c.Q). Ces nom et prénom sont consignés dans un acte d'état civil conservé par le directeur de l'état civil. Lui seul a la charge de dresser les actes de l'état civil, d'en tenir un registre et d'en assurer la publicité (art. 103 C.c.Q).

Attribut de la personnalité et reflet de la personne, le nom n'a cependant pas le caractère immuable auquel on pourrait s'attendre. Ainsi, en certaines circonstances exceptionnelles, ce nom peut parfois être changé avec le consentement d'un tribunal ou du directeur de l'état civil (art. 57 et ss. C.c.Q.). Par ailleurs, l'obligation qui est faite à chaque personne d'exercer ses droits civils sous le nom qui lui est attribué à la naissance, n'empêche pas une personne d'utiliser un autre nom en d'autres circonstances (art. 56 C.c.Q.). Cette situation, on le sait, se rencontre fréquemment dans le cas d'artistes dont les noms de théâtre sont souvent beaucoup mieux connus que les noms de baptême. L'utilisation d'un nom autre que celui attribué à la naissance n'est toutefois pas sans réserve. En effet, la personne qui utilise un nom autre que le sien est responsable de la confusion ou du préjudice qui peut en résulter.

L'identification

L'identification est l'action d'identifier, c'est-à-dire de reconnaître une personne, à certains traits non équivoques. L'identification est un processus d'information par lequel on compare de l'information afin d'avoir le degré de certitude requis à l'égard des qualités de la personne avec laquelle on entre en contact. C'est pourquoi on utilise dans certains milieux la notion d'authentification. Ainsi, dans la terminologie de l'informatique la notion d'authentification renvoie aux mécanismes tendant à procurer le niveau recherché de certitude à l'égard de l'identité d'une personne.

L'identification ne réfère pas toujours à l'identité légale et la multiplicité des rapports humains emporte une diversité des besoins en matière d'identification. Le processus d'identification des personnes peut prendre diverses formes.

Dans les environnements de transactions électroniques comme dans le monde physique, l'identification est un processus inhérent à la vie sociale, il est tributaire du contexte et du genre de transaction et il comporte des risques qu'il est nécessaire de gérer correctement.

Un processus inhérent à la vie sociale

L'identification est un processus inhérent à la vie sociale. Pour assurer le déroulement de la plupart des activités, tous doivent procéder à l'identification des personnes physiques, des personnes morales et des choses. Il est en effet essentiel, pour la plupart des interactions humaines, de savoir, à des degrés variables, à qui l'on a affaire.

Pour effectuer les comparaisons inhérentes à l'identification et pour obtenir le degré recherché de certitude, on aura besoin de plus ou moins d'informations. Il sera parfois

nécessaire d'avoir recours à des mécanismes de validation ou de corroboration des informations pouvant permettre d'accroître le degré de certitude à l'égard de l'identité d'une personne.

Un processus tributaire du contexte et du genre de transaction

Les relations que nous entretenons avec les autres sont variées : elles vont du simple salut au voisin que l'on reconnaît en raison de l'heure à laquelle il passe, jusqu'aux procédures complexes destinées à compléter une transaction importante.

L'identification est un processus qui n'est pas uniforme car le besoin d'identifier et de s'identifier est plus ou moins considérable selon les contextes[1]. On ne prend pas le même degré de précaution pour identifier nos vis-à-vis pour tous et chacun des contacts que l'on décide de faire. Certaines relations ont des enjeux plus importants que d'autres. Des transactions comportent des risques élevés tandis que d'autres portent peu à conséquence.

Ainsi, lors de rencontres dans un même lieu, l'identification d'un voisin ou d'un collègue de travail ne nécessite pas le recours à l'identité légale des personnes : on ne réclame pas sa carte d'identité à une personne pour les moindres contacts que l'on a avec elle! Bon nombre des transactions que nous faisons dans la vie courante ne supposent pas un niveau très élevé de certitude quant à l'identification. Par exemple, l'achat d'un journal au coin de la rue ne suppose pas pour le marchand et le client d'avoir mutuellement connaissance de leur identité respective. Il en va de même de la plupart des transactions dont le paiement s'effectue sur place et en argent comptant.

Certaines circonstances, par exemple l'exercice des droits d'accès à des informations personnelles ou encore la conclusion de contrats d'importance ou dont le paiement est différé, imposent toutefois un niveau de fiabilité plus élevé quant à l'identité des personnes impliquées. Ce phénomène met en lumière le fait que l'identification s'inscrit dans une logique de gestion des risques.

L'identification n'est pas un phénomène univoque : les situations dans lesquelles il est nécessaire d'identifier sont multiples. Le plus souvent, l'identification est volontaire mais elle est parfois une condition de l'obtention d'un bien ou d'un service. Sur Internet, l'identification peut se faire à l'insu de l'intéressé. Enfin, en certaines circonstances, elle est faite de force.

L'identification volontaire est celle que l'on fait spontanément afin d'établir qui l'on est auprès d'une autre personne. Par exemple, on parle de l'identification-condition lorsque l'obtention d'un bien ou d'un service est assujettie à un processus déterminé d'identification.

---

1 Matthew D. FORD, «Identity Authentication and 'E-Commerce'», 1998 (3) *The Journal of Information, Law and Technology (JILT)*. http://www.law.warwick.ac.uk/jilt/98-3/ford.html.

En ayant recours à divers moyens, il est possible d'identifier à son insu une personne qui visite un site ou prend part à une transaction sur Internet. Une politique d'identification doit impérativement baliser de telles pratiques car elles peuvent contrevenir aux lois sur la protection de la vie privée. Enfin, l'identification forcée est celle que doivent faire les forces de police dans l'accomplissement de leurs fonctions de lutte contre le crime.

Toutes ces démarches relatives à l'identification comportent des risques.

Un processus comportant des risques qu'il faut gérer

Ne pas identifier adéquatement comporte des conséquences. Si l'on identifie en exigeant trop d'informations, l'on s'expose à contrevenir aux règles en matière de protection de la vie privée. Si l'on recueille des informations insuffisantes, l'on peut devoir répondre des pertes, dommages et inconvénients qui pourraient résulter des erreurs engendrées par une identification inadéquate.

À l'égard de toute activité comportant des risques, quatre attitudes sont possibles : accepter les risques, éviter les risques, les réduire ou les transférer. Mais pour accepter les risques, il faut les connaître et en apprécier l'ampleur et la portée. Pour les éviter, il faut les connaître de même que les précautions, méthodes et processus par lesquels l'évitement est possible. Pour réduire les risques, il faut mettre en place les précautions afin de diminuer les dangers associés aux activités concernées. Enfin, pour transférer les risques, il faut les identifier et les porter à la connaissance de celui sur lequel on se propose de les faire porter.

La gestion des risques liés à l'identification est plus efficace si elle s'effectue méthodiquement et suivant une démarche qui tient compte des exigences des lois et des principes déontologiques applicables en matière d'identification des personnes.

La démarche proposée

Ce guide expose comment déterminer les risques afférents à l'identification et à mettre en place les politiques et processus afin d'accepter, éviter, réduire ou transférer les risques liés à l'identification dans un environnement de transaction électronique.

Afin de décider de manière adéquate des mécanismes et processus d'identification dans un environnement de transactions électroniques, il est nécessaire de suivre une méthode. Il faut se poser un ensemble de questions et y apporter des réponses dans l'ordre approprié.

Ainsi, il faut premièrement situer le besoin d'identification, i.e. répondre à la question : pourquoi doit-on identifier?

Deuxièmement, il faut spécifier le niveau de certitude requis quant à l'identité du co-contractant.

Troisièmement, il faut considérer les limites à la capacité d'identifier. Il est en effet fréquemment nécessaire de respecter un équilibre entre d'une part, les impératifs de certitude, voire de sécurité des transactions et, d'autre part, les exigences en matière de

protection de la vie privée des personnes. Autrement dit, on ne peut exiger un niveau de certitude pour l'identification au point de porter atteinte au droit à la vie privée d'une personne.

Une fois ces étapes accomplies, il est possible de sélectionner les mécanismes et processus d'identification qui répondront à la fois aux besoins de certitude tout en respectant les exigences relatives au respect de la vie privée des personnes.

Enfin, on passe en revue les méthodes et les processus à suivre afin d'attribuer une identité à une personne dans un environnement électronique.

Les étapes du processus de détermination des besoins et des moyens d'identification

Première étape :	La spécification des besoins d'identification
Seconde étape :	La détermination du degré de certitude requis pour l'identification
Troisième étape :	La considération des limites à la collecte et au traitement de l'information personnelle
Quatrième étape :	La détermination des mécanismes et processus d'identification, i.e. procéder au choix de la méthode d'identification

1. Première étape : Spécifier les besoins d'identification

Dans la vie sociale, comme dans les rencontres face à face, l'identification informelle et le contexte suffisent généralement à répondre à la plupart des besoins d'identification.

Il y a même des situations où l'on se passe de l'identification. Par exemple, dans le monde physique, on réclame rarement l'identification du co-contractant pour des transactions au comptant impliquant des sommes modiques se complétant en une seule étape.

Il est toutefois des situations où le besoin d'identification se révèle plus impératif. Par exemple, pour assurer la protection de la personne, le pharmacien exigera de celui qui présente une ordonnance médicale qu'il s'identifie. L'identification pourra alors servir à vérifier d'éventuelles incompatibilités entre médicaments.

Dans d'autres cas, il s'agit de connaître l'identité afin de pouvoir éventuellement contacter la personne dans le cas où elle omettrait de remplir l'une de ses obligations. Par exemple, il peut être utile d'être en mesure contacter la personne qui ne paie pas son dû. L'identité sera aussi nécessaire pour accepter de donner accès à des renseignements qui sont accessibles seulement à la personne concernée. Par exemple, pour autoriser l'accès au dossier fiscal d'une personne.

Les organisations gèrent souvent une relation personnelle avec un citoyen. Dans la perspective de fournir leurs services selon une approche orientée client, elles jugeront

parfois opportun de n'utiliser qu'un identifiant pour tous les dossiers détenus au sujet d'une personne.

Mais la plupart du temps, identifier n'est généralement pas une fin en soi : c'est parfois une formalité imposée par la loi ou découlant des devoirs généraux de prudence. Au surplus, c'est un processus tributaire du degré de certitude requis en fonction du contexte, de l'importance de la transaction et de l'ensemble des circonstances dans lesquelles l'interaction se déroule. Ce dernier aspect fait l'objet de la seconde étape.

1.1 Pourquoi identifier?

La première question que doivent se poser les personnes responsables de la mise en place et de la gestion de sites ou d'environnements électroniques dans lesquels se déroulent des transactions est la suivante : Sommes-nous en présence d'une situation où l'identification de la personne est nécessaire?

Il faut donc distinguer les situations où l'identification n'est pas nécessaire de celles où elle est nécessaire.

Grille de questions

- L'identification est-elle nécessaire ou non?
  - Pourquoi?
  - La loi ou un règlement l'exige? i.e., existe-t-il une obligation de s'identifier? ou un devoir d'identifier?
  - Un devoir de prudence l'exige? Les circonstances et les risques liés aux transactions envisagées (décrire) imposent-ils un devoir de s'identifier? ou un devoir d'identifier?
- **Si OUI ➔ La situation nécessite l'identification**
- **Si NON ➔ La situation ne nécessite pas l'identification**

1.2 Les situations où l'identification n'est pas nécessaire

Ce ne sont pas toutes les transactions qui nécessitent l'identification des parties. Ainsi, dans le monde physique, une personne voulant acheter un journal ou un livre ou se procurer des vêtements ou des articles de bureau n'a, a priori, aucune obligation de révéler son identité. Les seuls éléments essentiels pour que la transaction s'accomplisse, dans ce cas, sont le paiement du bien et sa livraison.

Il n'est pas toujours nécessaire non plus d'identifier la personne qui fait un paiement. La loi permet que le paiement soit effectué par toute personne même si celle-là n'est pas la vraie débitrice de l'obligation de paiement (art. 1555, al 1 C.c.Q.). Par exemple A s'abonne à un fournisseur de services Internet mais c'est B qui paie sa facture à la fin du mois. Il importe peu au fournisseur de services Internet qu'il soit payé par A ou par B et donc il ne lui sera pas nécessaire de procéder à l'identification de celui qui paie.

Dans le cyberespace, le besoin d'identifier peut exister dans des situations où il n'est guère ressenti dans les situations analogues se déroulant dans l'espace physique.

Par exemple, dans l'espace physique, l'apparence d'une personne peut suffire à l'identifier. Les co-contractants peuvent la reconnaître sans même qu'elle ait à décliner son nom. Dans une telle situation, il y a eu identification lors de la transmission d'information inhérente à la rencontre dans un même lieu physique. Une telle identification est habituellement impossible dans le cyberespace.

Il importe toutefois d'être en mesure d'expliquer pourquoi le contexte d'une transaction électronique nécessite d'identifier alors que cette nécessité n'est pas ressentie dans le monde physique.

Les questions suivantes aideront à effectuer cette détermination :

- Quels sont les risques inhérents à la transaction?
- Ces risques sont-ils modifiés du fait que la transaction se déroule en environnement électronique?
- Les risques sont-ils tels qu'ils justifient d'identifier positivement le co-contractant?

De façon générale, s'il est impossible de trouver une bonne raison de collecter des informations identifiantes, il faut tenir pour acquis que l'identification n'est pas nécessaire. Dans pareille situation, les lois sur la protection des renseignements personnels et les principes de protection de la vie privée interdisent de collecter des informations personnelles.

1.2.1 Les situations où l'identification reste possible

Même si elle n'est pas formellement effectuée, l'identification demeure généralement possible, soit de façon directe ou indirecte. Il est en effet usuel de rappeler que dans le cyberespace, toutes les transactions laissent des traces.

Lorsque la transaction ne requiert pas l'identification, se pose alors la question de savoir s'il faut conserver des informations susceptibles d'être utilisées afin de retracer la personne concernée pour les rares cas où cela s'avérerait nécessaire.

Si on n'est pas en mesure de préciser un besoin de collecter et de conserver une information identifiante, il faut alors s'assurer que ces informations ne sont pas traitées ou conservées.

Les questions suivantes aideront à déterminer s'il y a des situations pour lesquelles il serait nécessaire de retracer la personne concernée :

- Existe-t-il des circonstances pour lesquelles il serait nécessaire de retracer ou d'identifier une personne ayant effectué une transaction?
- Quelle est la fréquence prévisible de la survenance de telles circonstances?
- L'existence de telles circonstances a-t-elle pour conséquence de rendre <u>nécessaire</u> la collecte et la conservation d'informations identifiantes?

1.2.2 Les situations où l'identification est habituellement impossible : l'anonymat

Il y a des circonstances où non seulement l'identification n'est pas nécessaire mais en plus, elle s'avère impossible. En pratique, lorsqu'on se trouve dans une situation dans laquelle il est nécessaire d'identifier le co-contractant, il ne pourra être question d'anonymat. On parle d'anonymat lorsqu'une transaction se fait ou peut se faire licitement, sans l'identification de l'un des participants.

Il existe présentement deux grandes approches pour protéger l'anonymat dans les environnements électroniques :

- les serveurs anonymisateurs et
- le chiffrement (ou le cryptage).

Les serveurs anonymisateurs permettent de naviguer sur Internet ou d'envoyer un message de courrier électronique sans divulguer l'identité de l'usager. Ainsi l'usager cache son identité en faisant transmettre ses messages ou ses commandes de navigation par un serveur anonyme.

Il existe deux types de communications qui garantissent l'anonymat :

- l'anonymat identifiable et
- l'anonymat non identifiable.

Il y a anonymat identifiable lorsque le serveur anonyme ne donne au destinataire aucun indice quant à l'identité de l'usager mais laisse cette information entre les mains d'un tiers unique. Le destinataire du message pourrait identifier l'auteur du message en convainquant le tiers, ayant anonymisé le message de l'auteur, de lui révéler l'identité de ce dernier. Cette information, si elle n'a pas été effacée, pourrait également être obtenue par le destinataire du message au moyen d'un ordre d'un tribunal. Cette façon d'anonymiser les messages offre une protection relative de l'anonymat. Mais elle pourra souvent s'avérer suffisante, quoiqu'elle implique une certaine dose de confiance envers l'opérateur du système anonymisant qui pourrait copier, lire ou révéler le message à des tiers[2].

Lorsqu'on parle d'anonymat non identifiable, on fait référence à une communication dont l'auteur ne peut être, en principe, identifié. La technologie présentement utilisée sur Internet permet ce type de communications au moyen de l'envoi du message à travers une chaîne de serveurs anonymes[3]. Sommairement, cette technique consiste à chiffrer le message en différentes couches à l'aide de la clé publique du destinataire, chacune contenant l'adresse du destinataire suivant et ne pouvant être déchiffré par lui qu'à l'aide de sa clé privée. Le message est ensuite expédié à un premier serveur anonyme. Celui-ci anonymise la

---

2 Voir A. Michael FROOMKIN, «Anonymity and its Enmities», (1995) *J. Online L.,* art. 4, par. 14 et suiv., disponible à http://www.law.cornell.edu/jol/froomkin.htm

3 Voir au même effet Anne Wells BRANSCOMB, «Anonymity, Autonomy and Accountability : Challenges to the First Amendment in Cyberspace», (1995) 104 *Yale L.J.* 1639, 1643.

communication, décode la partie du message qui lui est destiné, c'est-à-dire l'adresse du prochain destinataire, et lui expédie. Cet autre serveur, lorsqu'il reçoit la communication, efface également l'en-tête permettant l'identification et décode la partie de la communication qui lui est destinée, c'est-à-dire l'adresse du prochain destinataire. Il réexpédie ensuite le message et la chaîne se poursuit. Aucun des intermédiaires de la chaîne ne pouvant décoder plus que la partie du message qui a été encrypté à son attention, le corps du message parvient finalement à son véritable destinataire qui peut le décoder à l'aide de sa clé privée. Cette technologie diminue considérablement les risques d'être retracé. Elle peut être utilisée afin de couvrir des comportements illicites comme la conspiration, la diffamation, la propagande haineuse, etc.

Enfin il existe la notion de pseudo-anonymat qui se définit comme le fait pour un usager d'utiliser un pseudonyme dans ses relations et ses transactions avec les autres usagers. De la même façon que l'anonymat, ce pseudo-anonymat peut être non identifiable ou identifiable[4]. Une personne utilisant un pseudonyme non identifiable sur l'Internet pourrait fort bien en arriver à créer une personnalité électronique distincte de sa personne[5], avec une réputation et une image. Le chiffrement et l'utilisation de la signature électronique peuvent même servir à assurer l'intégrité de cette pseudo-personne en ce qu'ils permettent de s'assurer que personne d'autre n'enverra de messages au nom de cette dernière. Dans le cas d'un pseudonyme identifiable, il est possible d'en arriver ultimement à connaître la véritable identité de l'auteur d'une communication. Cette option a cependant l'avantage de permettre au récepteur de la communication d'y donner suite directement, en affichant sa réponse dans le courrier électronique de la pseudo-personne. Ce serveur, qui conserve un relevé de la véritable identité de chaque usager, pourrait cependant être obligé de la divulguer, conformément à un ordre d'un tribunal par exemple, d'où le caractère identifiable de ce type de pseudo-anonymat[6].

L'anonymat et le pseudo-anonymat

Avantages	Inconvénients
- garantit la protection de la vie privée, notamment des renseignements personnels - facilite la communication sans être identifié - favorise la liberté d'expression	- favorise les activités frauduleuses - favorise la perpétration des crimes et des activités illégales - encourage la diffamation en exonérant l'expéditeur d'un message de responsabilité

4 A. Michael FROOMKIN, «Anonymity and its Enmities», (1995) *J. Online L.,* art. 4, par. 31 et suiv., disponible à http://www.law.cornell.edu/jol/froomkin.htm

5 Voir : Pierre TRUDEL et France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997,p. 2 et ss; KARNOW, C.A., «The Encrypted Self : Fleshing Out the Rights of Electronic Personnalities», (1994) 8 *Journal of Computer & Information Law* 1 et suiv.

6 A. Michael FROOMKIN, «Anonymity and its Enmities», (1995) *J. Online L.,* art. 4, par. 33 et suiv., disponible à http://www.law.cornell.edu/jol/froomkin.htm

L'identification de l'usager n'est pas toujours nécessaire pour la prestation d'un service ou la conclusion d'une transaction. Pour d'autres services ou transactions, il importe peu qu'on s'identifie sous son vrai nom ou un nom qui s'avère faux. Dans ces cas, l'utilisation du pseudo-anonymat est utile. Par exemple, lorsqu'on veut se joindre à une liste de discussion, on peut s'identifier sous un faux nom sans que cela ait d'importance pour le site offrant ce service ou les autres usagers. Ainsi, en utilisant un nom d'usager, on protège notre vie privée tout en permettant notre repérage par le service et par les autres usagers.

On voit donc qu'il existe des situations dans lesquelles il n'y a pas lieu de s'assurer de l'identité de l'usager selon un niveau quelconque de fiabilité. Par ailleurs le site qui décide d'accepter l'utilisation de l'anonymat ou du pseudo-anonymat devra prendre en considération les désavantages de cette pratique.

L'anonymat n'est acceptable que pour les services et les transactions pour lesquels il n'existe pas le besoin d'une identification ou pour lesquels l'identification peut être faite sans qu'il soit nécessaire d'assurer un niveau de fiabilité quelconque.

1.3 Les situations où l'identification est nécessaire

L'identification peut être nécessaire. Il existe en effet des transactions dans lesquelles l'identification d'une partie est nécessaire :

1- Lorsque la transaction ne peut être conclue que par une personne déterminée.

Par exemple :

- L'achat d'un médicament sur Internet pour lequel une ordonnance médicale est requise ne pourra être fait que par la personne à laquelle ce médicament a été prescrit.
- L'accès à un dossier contenant des renseignements personnels. La loi protège la confidentialité des renseignements personnels et seule la personne concernée a le droit d'accès à ces renseignements. Le détenteur des renseignements personnels sur autrui doit s'assurer de l'identité de la personne désirant accéder au dossier afin d'empêcher la divulgation des données personnelles à des tiers non autorisés. Lorsqu'un dossier médical est constitué sur la personne A, les informations contenues au dossier sont confidentielles et seulement A a le droit de consulter ce dossier. Si une personne demande d'accéder à cette information, l'hôpital devra s'assurer que c'est bien A qui fait la demande ou une personne autorisée par elle.

2- Lorsque la transaction ne peut être conclue que par un groupe de personnes déterminé.

Par exemple :

- Un service de courrier électronique n'est offert qu'aux résidents du Québec. La personne voulant s'inscrire à ce service devra prouver le fait qu'elle habite au Québec.

- Un service de courrier électronique pourrait n'être offert qu'aux étudiants de l'Université de Montréal. Dans ce cas, la personne s'inscrivant à ce service devra prouver qu'elle est de cette université.

3- Lorsque la transaction implique la vente d'un produit interdit à certaines personnes.

Par exemple :
- L'achat de boissons alcooliques et de cigarettes par des mineurs.
- L'achat de produits destinés strictement aux adultes. Une personne voulant commander en ligne une revue ou une cassette contenant du matériel réservé aux adultes devra démontrer son âge.

4- Lorsque la transaction implique la transmission d'informations à caractère confidentiel.

Par exemple :
- Lors d'une déclaration d'impôt en ligne, il est essentiel d'identifier avec précision la personne. Si on omet de faire une telle identification, il existe un risque de fraude ou que l'identité soit usurpée.
- Lors de l'opération d'un service de courtage en ligne, permettant d'acheter et de vendre des actions à la Bourse par Internet, il est essentiel de s'assurer que la personne qui place la commande d'achat ou de vente des actions est bien le titulaire du compte opéré.

On constate que la plupart du temps, une personne doit démontrer une qualité pour obtenir un bien ou un service ou pour confirmer son droit à quelque chose. Mais indépendamment de ces circonstances, l'obligation d'identifier peut découler d'un devoir imposé par une loi ou découler du devoir général de prudence et de diligence.

Plusieurs lois fédérales et québécoises prescrivent l'identification préalable des citoyens lors d'échanges avec un organisme du secteur public ou du secteur privé. Toutefois, ce devoir d'identification n'incombe pas toujours aux organismes publics ou privés. Souvent, c'est le citoyen qui doit fournir la preuve de son identité afin de faire valoir ses droits. Par ailleurs, les lois ne sont pas toujours claires quant à la façon dont l'identité doit être déclinée et les exigences varient.

Le plus souvent, l'obligation d'identifier ou de s'identifier procède du devoir général de prudence incombant à toute personne raisonnable. Ainsi selon le Code civil du Québec,[7] toute personne doit se comporter en personne raisonnable compte tenu des circonstances.

---

7 Voir l'article 1457 du Code civil du Québec qui édicte que :

Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.

Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.

Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde.

En vertu de ce devoir, dont l'existence et l'ampleur est fonction des circonstances, une personne peut se voir imposer l'obligation d'identifier l'autre partie. L'ampleur de ce devoir est fonction des risques inhérents à l'activité concernée.

Pour déterminer si la prudence emporte une obligation d'identifier, il faut se demander si dans des circonstances semblables, une personne raisonnable aurait trouvé nécessaire d'identifier l'autre partie. La signification concrète du standard de «personne raisonnable» est déterminée en fonction des circonstances particulières de chaque situation. Baudouin[8] écrit à ce sujet que :

> [Il faut] *comparer la conduite de l'agent à celle d'une personne normalement prudente et diligente, douée d'une intelligence et d'un jugement ordinaires, et se demander si elle aurait pu prévoir ou éviter l'événement qui a causé le dommage. Il ne s'agit pas d'obliger l'individu à prévoir tous les types d'accidents possibles, mais seulement ceux qui, dans les circonstances, sont raisonnablement probables. La notion de «bon père de famille», d'«honnête citoyen», de «personne prudente et diligente», varie selon des impératifs de temps et de lieu. Les changements sociaux, l'évolution des mœurs affectent la physionomie générale de ce modèle constamment remis en question par l'appréciation souveraine qu'en font les tribunaux, dans chaque cas particulier.*

Il faut également tenir compte des circonstances particulières d'une transaction électronique. Ainsi un paiement en ligne diffère d'un paiement au guichet d'une institution financière même s'il s'agit de la même opération juridique. Pour déterminer s'il existe une obligation d'identifier, il faut se reporter aux circonstances du paiement; de quelle façon celui-ci est-il effectué, quel est le montant en cause, quelles sont les mesures de sécurité mises en place, etc. On doit se demander de quelle manière agirait une personne raisonnable dans un environnement électronique face à une même situation. À cet égard, il importe de tenir compte des usages ayant cours dans le commerce électronique.

Si on arrive à la conclusion que dans ces mêmes circonstances, une personne raisonnable aurait procédé à l'identification de l'autre partie, il faut tenir pour acquis que le devoir d'identification existe.

À défaut de se comporter conformément à cette norme de la personne raisonnable, on aura à répondre des dommages qui pourraient résulter d'un pareil comportement.

Évidemment, le devoir d'identification trouve ses limites dans celui de respecter la vie privée d'autrui. Ainsi dans une situation donnée une personne raisonnable pourrait juger que l'identification de l'autre partie, même si elle pourrait être utile ou nécessaire, porte atteinte au droit à la vie privée. Dans ce cas, l'obligation d'identification doit être comprise

---

8 Jean-Louis BAUDOUIN, *La responsabilité civile*, 4é édition, Les Éditions Yvon Blais Inc., 1994, p.95 §132.

comme emportant celle de prendre des mesures afin de protéger la vie privée de la personne.

1.3.1 Les situations où une personne doit s'identifier

Il y a des situations où une personne a le devoir de s'identifier. Soit que ce devoir découle d'une obligation explicitement prévue dans une loi, soit qu'elle découle de la nature même de la situation dans laquelle elle se trouve.

a) L'obligation explicite de s'identifier

Il existe en droit québécois et canadien des dispositions qui imposent un devoir absolu d'identification des individus. Ces obligations sont tellement importantes que le fait de ne pas s'y conformer peut entraîner des conséquences graves et engager la responsabilité de la personne qui devait s'assurer de l'identité d'un individu.

La loi oblige dans certains cas une personne à s'identifier (voir en Annexe 1, Tableau 1 - *Exemples de l'obligation de s'identifier en vertu de la loi*). D'une part, il y a les lois imposant une vérification préalable de l'identité pour contrer la présence de mineurs dans certains endroits ou pour leur interdire la consommation de certains produits. Ainsi un mineur doit s'identifier pour entrer dans un bar ou pour acheter de l'alcool.

D'autre part, la loi accorde le pouvoir de procéder à une identification aux personnes en charge d'assurer l'ordre et la paix publique (les agents de la paix). Ainsi l'agent de la paix qui a des motifs raisonnables de croire qu'une personne a commis une infraction peut exiger qu'elle lui déclare ses nom et adresse afin que soit dressé un constat d'infraction (*Code de procédure pénale*, L.R.Q., c. C-25.1, art. 72 et 74). Cependant, ces pouvoirs sont accompagnés d'une exigence qui consiste à remettre en liberté un individu dès qu'il a confirmation de son identité (voir l'article 24 de la *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, qui affirme que «nul ne peut être privé de sa liberté et de ses droits […]»).

La *Loi sur l'identification des criminels* oblige les personnes déclarées coupables d'un acte criminel à coopérer à certains actes d'identification (comme la «prise d'empreintes digitales, des photographies et de toute autre mensuration ainsi que tout autre opération anthropométrique», L.R.(1985)., ch. I-1, art. 2).

b) Le devoir de s'identifier découlant des circonstances

Il existe des situations où une personne doit s'identifier parce que la nature de la situation le commande. Voici quelques exemples :

(1) pour mener à bon terme une transaction.

- une personne doit divulguer son adresse pour que la livraison du produit acheté puisse être effectuée. Par exemple, lors d'un achat en ligne d'un livre, le site vendeur doit connaître l'adresse de l'acheteur afin de pouvoir lui expédier le livre acheté.

(2) pour offrir une garantie quant au paiement de la transaction.

- un bien ou un service peut être livré sur la simple divulgation d'un numéro de carte de crédit. En supposant que cette carte a été volée, son vrai propriétaire en empêchera le paiement. Face à une telle situation, le vendeur doit disposer des coordonnées de l'acheteur (nom et adresse) pour pouvoir réclamer le paiement ou reprendre son bien.

(3) lors d'une inscription à un service devant être livré à une adresse (physique ou électronique) particulière, afin de pouvoir exécuter l'obligation.

- lorsque A s'inscrit à un club en ligne qui s'engage à lui transmettre chaque semaine des nouvelles concernant les activités du club, A devra divulguer son adresse électronique pour que les informations lui soient transmises.

(4) lors d'une inscription à un service pour garantir l'exécution des termes du contrat.

- A s'inscrit à un service de courrier électronique dont les termes du contrat prévoient que si l'usager utilise le service pour faire du «spamming», une amende de 5$ par message sera imposée. Pour appliquer cette sanction, le fournisseur de courrier doit connaître le nom et l'adresse de l'usager. Si le contrat interdit en plus à la personne d'utiliser le service dans le futur, il est nécessaire de l'identifier lors de son inscription pour s'assurer qu'elle ne tente pas de se réinscrire au service.

Dans ces situations, l'obligation faite à une personne de s'identifier est une condition inhérente au succès de la transaction. Pour que cette dernière soit possible et être complétée, il faut que la personne s'identifie. En outre, le degré d'identification exigée de la personne est habituellement fonction des exigences intrinsèques de la transaction considérée.

1.3.2 Le devoir de s'assurer de l'identité d'une personne

Il est ici question des situations dans lesquelles une autorité publique ou une entreprise a le devoir d'identifier une personne ou de vérifier son identité.

Les lois fédérales et québécoises comportent différentes dispositions concernant l'identification des individus; il convient de présenter les différentes situations dans lesquelles il y a un devoir de s'assurer de l'identité d'une personne. Ce devoir peut aussi découler de la nature de la transaction.

a) Le devoir expressément prévu d'identifier

Il s'agit des situations où il y a une obligation explicite d'identifier. En certaines circonstances, des lois prescrivent à des personnes expressément désignées une obligation formelle d'identifier. Il faut distinguer entre l'identification attestée par une personne et l'identification attestée par un officier public.

Certaines dispositions législatives obligent la révélation de l'identité sans faire plus de précision. Ces dispositions sont rédigées en termes généraux, laissant une grande discrétion quant à la façon dont l'identité doit être établie. Par exemple, en vertu de la législation québécoise sur la protection des renseignements (secteurs public et privé), un individu peut accéder aux renseignements le concernant s'il procède par écrit et s'il fournit une preuve justifiant de son identité.

Dans les lois en vigueur au Québec, on trouve des dispositions qui imposent des devoirs généraux aux citoyens ou aux autorités publiques en matière d'identification. Les tribunaux reconnaissent en principe qu'«Il n'est que normal, voire même nécessaire, qu'un pouvoir d'État exerce un contrôle de l'identité de ses citoyens et citoyennes et qu'il s'assure de pouvoir les individualiser»[9].

(1) Aux termes de certaines lois, le citoyen n'a pas la possibilité de refuser de fournir des renseignements si l'État affirme en avoir besoin pour ses programmes. Par exemple, pour déclarer son revenu aux fins de l'impôt ou pour répondre aux questionnaires de recensement.

(2) Le citoyen conserve une faculté de refuser de fournir des renseignements d'identification à certains services gouvernementaux, dans la mesure où il en accepte les conséquences. Par exemple ne pas recevoir de prestations gouvernementales telles les prestations d'assurance-emploi, un permis de conduire, etc.[10].

(3) Certaines lois posent des exigences particulières relativement au statut d'une personne afin qu'elle puisse bénéficier de certains droits. Alors, l'identification est nécessaire afin de vérifier si la personne rencontre ces exigences. À titre d'exemple, pour obtenir un changement de nom, une personne doit détenir la citoyenneté canadienne et présenter une preuve de citoyenneté comme un passeport ou un certificat de citoyenneté.

(4) D'autres lois obligent explicitement la vérification de l'identité des personnes afin de préserver les garanties qu'offrent certains documents (notamment le cas des notaires qui sont tenus d'attester qu'ils ont vérifié l'identité des personnes lors de certaines transactions).

(5) Certaines lois exigent un degré plus élevé de fiabilité dans l'identification d'un individu. Par exemple, les lois électorales où l'individu devra obtenir l'attestation de témoins ou prêter serment.

---

9 *Coté et St-Antoine,* [1991] R.D.F. 513 (C.A.); *Moulay Ali Benmansour c. Le Directeur de l'État civil et al.*, [1995] R.J.Q. 205 (C.S.); *Montreuil c. Société de l'assurance automobile du Québec*, J.E. 98-1988 (C.S.)

10 Groupe de travail sur les questions de droit, Chapitre 3 : Collecte et partage des renseignements personnels dans *Études des questions de droit entourant la sécurité des renseignements électroniques,* Canada, Ministère de la justice, 1996.

(6) Il y a quelques dispositions législatives qui exigent clairement que les individus soient identifiés préalablement à l'accomplissement de certains actes. Il s'agit d'une obligation ferme que doivent rencontrer les personnes expressément désignées par la loi.

(7) En matière de droit pénal et criminel, des dispositions permettent ou imposent une identification complète des individus qui ont commis un crime : utilisation des empreintes digitales, des résultats d'ADN etc.

b) Le devoir d'identifier découlant de la nature de la transaction

Les transactions en ligne impliquent généralement la communication de certaines informations identifiant une partie, même de manière minimale, afin par exemple, de livrer le produit et de procéder à la facturation s'il y a lieu, tels les transactions par téléphone (achats par téléphone) ou l'accès à certains services (abonnement aux services publics comme le téléphone ou l'électricité, inscription à des cours).

L'identification est souvent nécessaire pour avoir accès au dossier d'une personne. Par exemple, pour renouveler son permis de conduire, l'agent doit être en mesure de vérifier au dossier si celui-ci est réellement en droit d'obtenir ce renouvellement.

*** * ***

On retiendra de cette première étape que l'identification n'est pas toujours nécessaire. Comme c'est une activité entraînant des conséquences à l'égard des personnes et pour l'organisme, il importe de bien s'assurer qu'elle est nécessaire; soit qu'elle est exigée par les lois ou elle découle des exigences de la prudence ou de la bonne gestion.

Aussi, lors de cette première étape, il importe de déterminer si l'identification est nécessaire et de spécifier en vertu de quoi elle l'est. La ligne de conduite la plus avisée consiste à toujours être en mesure d'expliquer pourquoi telle ou telle information est requise lors du processus d'identification.

À défaut de documenter ce qui peut parfois relever des habitudes ou de l'évidence, il pourra être difficile de choisir les moyens les plus adéquats et les moins intrusifs afin de répondre aux impératifs d'identification. Alors, on accroît les risques de se trouver en contravention avec les exigences en matière de protection de la vie privée des personnes.

2. Deuxième étape : Déterminer le degré de certitude requis pour l'identification

Au cours de cette seconde étape, il s'agit de répondre à la question «Quel est le degré de certitude requis pour l'identification?».

Compte tenu des enjeux et des risques des transactions qui seront réalisées dans l'environnement considéré, il faut ici spécifier le degré de certitude dont on a besoin en matière d'identification.

L'identification est un processus destiné à réduire l'incertitude. Ce processus vise à procurer la quantité optimale d'information à l'égard d'une personne afin de pouvoir procéder à la transaction avec un niveau de risque acceptable. Cet aspect est mis en lumière par Matthew Ford qui parle d' «identity authentication»[11]. Dans le langage de l'informatique, c'est souvent la seule dimension qui est prise en considération. Lorsqu'on parle d'authentification, on fait référence aux moyens afin de procurer le degré requis de certitude à l'égard de l'identité d'une personne.

Dans un environnement de transactions, on va requérir plus ou moins d'information selon que l'on se propose de contracter avec un inconnu ou avec une personne que l'on connaît de longue date. De la même façon, plus la transaction envisagée comporte des enjeux importants, plus on voudra disposer d'informations afin de s'assurer de l'identité du co-contractant. Inversement, pour les transactions à enjeu mineur ou dérisoire ou encore lorsque l'identité du co-contractant n'a pas d'importance, on ne va pas consacrer de grands efforts afin d'obtenir les informations relatives à l'identité du co-contractant. Dans ce dernier cas, l'analyse que l'on fait des risques de la transaction porte à conclure qu'il suffit d'un minimum d'informations.

Pour obtenir le degré recherché de certitude, on aura besoin de plus ou moins d'informations. Il sera parfois nécessaire d'avoir recours à des mécanismes de validation ou de corroboration des informations pouvant permettre d'accroître le degré de certitude à l'égard de l'identité d'une personne.

En somme, l'identification est une activité visant essentiellement à réduire ou gérer les risques inhérents à une transaction. Mais cela met également en lumière le fait que l'identification se présente sous plusieurs facettes puisque les transactions auxquelles nous prenons part ne sont pas toutes de même importance. Car s'il y a des risques à ne pas recueillir des informations identifiantes, la cueillette d'informations injustifiées entraîne elle aussi des risques. Ces risques sont envisagés dans la troisième étape.

---

11 Matthew D. FORD, «Identity Authentication and 'E-Commerce'», 1998 (3) *The Journal of Information, Law and Technology (JILT)*. http://www.law.warwick.ac.uk/jilt/98-3/ford.html.

Aussi, la gestion de l'identification se présente comme une composante de la gestion des risques afférents aux activités prenant place dans un environnement transactionnel donné.

2.1 La démarche

Il s'agit de déterminer quelle est l'information essentielle afin de pouvoir réaliser la transaction conformément aux exigences des lois, en tenant compte des enjeux et des risques qu'elle comporte et en respectant les préceptes et obligations de prudence et de diligence.

Il s'agit de procéder à l'analyse des transactions envisagées afin de déterminer, le plus précisément possible, quelles sont les informations identifiantes qui sont nécessaires. La tâche consiste essentiellement à opérationnaliser le principe de nécessité qui limite le droit de collecter des renseignements personnels.

La nécessité s'apprécie en fonction de facteurs tels que les enjeux et risques de même que les exigences spécifiques à la transaction. Au nombre des facteurs à considérer, il y a le montant en jeu, le degré de sensibilité des informations en cause ainsi que la protection du capital de crédibilité du site ou du service. Ces facteurs sont plus amplement expliqués ci-après.

2.1.1 Les enjeux de la transaction électronique

Le degré requis de certitude pour l'identification dépend au premier chef des enjeux de la transaction concernée. Ces enjeux peuvent être liés à la valeur, au montant de la transaction ou encore découler du degré de sensibilité de l'information échangée.

Le montant en jeu doit être examiné : lorsque les sommes sont modiques, se pose la question de savoir s'il vaut la peine de consacrer des ressources à l'identification pour des enjeux financiers modestes.

Le degré de sensibilité des informations en cause est aussi un facteur à considérer. On ne traite pas de la même façon des informations personnelles et des renseignements triviaux révélant peu de choses sur une personne.

La protection du capital de crédibilité du site ou du service est un autre facteur à considérer dans une analyse des risques : il se peut que les sommes en jeu lors de chaque transaction soient modestes et que les informations qui transitent soient insignifiantes. Mais une identification inadéquate pourrait engendrer des dysfonctionnements susceptibles d'entamer le capital de crédibilité de l'organisme.

Il n'y a pas *a priori* de raison d'exiger un *quantum* d'informations plus considérable pour des transactions d'importance et d'enjeux similaires pour le seul motif que l'une est réalisée sur Internet et l'autre dans un environnement supposant la présence physique des personnes impliquées.

Un bon guide est de fonder l'évaluation des enjeux en s'inspirant des évaluations qui sont faites à l'égard de transactions analogues dans le monde physique. Dans un second temps, on prend en considération les caractéristiques du contexte virtuel ayant un impact sur les enjeux de la transaction. On recherchera à dresser les équivalences appropriées afin de procurer les repères pertinents et procurant un niveau de certitude comparable à celui qui est généralement requis dans le monde physique.

2.1.2 Les risques de la transaction électronique

Outre les enjeux inhérents au type de transaction envisagée, il faut considérer l'existence de risques accrus tels que mascarade, répudiation des transactions et atteintes à la vie privée. Ces risques doivent être assumés dans les transactions électroniques et les mécanismes d'identification participent aux démarches de réduction des risques de transiger dans le cyberespace.

2.1.3 Les exigences spécifiques à une transaction donnée

Les lois ou les règlements peuvent imposer des exigences spécifiques pour une transaction donnée.

Par exemple

- Si elle ne peut avoir lieu qu'avec une personne spécifique
- S'il faut livrer

Il faut donc aussi examiner les nécessités intrinsèques de la transaction car ces exigences emportent généralement des impératifs accrus en termes de certitude et d'information.

2.2 L'évaluation des risques et enjeux de la transaction

Cette évaluation tient compte du contexte technique, juridique et circonstanciel dans lequel se déroule la transaction, notamment du degré de sécurité d'Internet.

Dans le secteur public, l'analyse des enjeux relatifs à l'identification peut présenter des différences avec celle qui peut être faite dans le secteur privé[12].

Une entreprise œuvrant dans le secteur privé pourra évaluer les risques associés à l'identification de ses co-contractants en termes de pertes financières. Par exemple, une banque prendra en compte le pourcentage de fraude et de perte des données associés à ses services et allouera un pourcentage de ses revenus pour assumer ses risques. Le pourcentage alloué pour la gestion de ses risques dépendra de la rentabilité de l'activité en

---

12 Voir: Jane Kaufman WINN, «The Hedgehog and the Fox : Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions», 51 :3 *Administrative Law Review*, 1999, pp.955, 959-960.

cause. Cette évaluation est nécessaire puisqu'une entreprise peut être poursuivie devant les tribunaux et donc tenue responsable pour la façon dont ses services sont offerts en ligne.

Par contre un organisme œuvrant dans le secteur public doit se soucier des conséquences financières et non financières de son activité. L'évaluation des risques reliés aux transactions ne peut procéder uniquement d'une analyse des dimensions financières de l'activité concernée ou du service.

Dans son analyse des risques afférents à l'identification, l'organisme public doit tenir compte des enjeux associés à son champ d'activité, de la sensibilité des informations ou des services qui sont en cause et des attentes des clientèles spécifiques.

Ces facteurs portent généralement plusieurs entités de service public à adopter des standards qui tiennent compte des attentes du public et pas seulement des risques spécifiques associés aux transactions.

La démarche doit procurer une évaluation la plus précise possible des risques qui découlent de l'identification, de la non-identification ou de l'identification inadéquate dans le cadre des transactions envisagées sur le site.

Ainsi, on pourra considérer qu'une transaction consistant à recueillir les coordonnées d'une personne afin de lui expédier un dépliant d'information sur un programme gouvernemental ne présente pas beaucoup de risques.

En revanche, si la transaction porte sur l'inscription d'une personne à un programme de prestations régi par une loi ou un règlement spécifiant des conditions d'admissibilité et autres exigences, la non-identification ou l'identification inadéquate comportera des risques qui pourront s'avérer considérables.

Ainsi, au TERME DE CETTE DÉMARCHE, on aura identifié les enjeux et risques de la transaction considérée et ce qui est nécessaire d'obtenir comme informations afin de disposer du degré de certitude que commandent ces enjeux et risques.

La réponse aux questions suivantes aidera à spécifier le degré requis de certitude dans un contexte donné :

➢ Quels sont les enjeux et les risques de la transaction? ➢ Quelles sont les conséquences de l'identification? de la non identification? De l'identification inadéquate?	• Conséquences financières? - valeur de la transaction? - valeur des autres inconvénients • Conséquences non financières? - confiance et crédibilité du service? - responsabilité, politique, juridique et administrative? ▪ Conséquences pour les parties impliquées? - pour la personne?

	- pour le service?

Selon les transactions, il y a différents degrés d'identification qui sont requis.

Le degré requis de certitude est habituellement fonction de l'enjeu et des risques de la transaction. Plus la transaction porte sur un enjeu important, au plan de la valeur et au plan de la sensibilité de l'information échangée, plus il faudra accroître le degré de certitude.

On peut caractériser la plupart des transactions intervenant dans un environnement électronique transactionnel en les situant sur une échelle fondée sur le degré requis de certitude à l'égard de l'identité de la personne co-contractante.

Une telle échelle est fonction des enjeux et des risques.

Enjeux	modestes	sensibles ou importants	très sensibles ou très importants
Risques	faibles	moyens	élevés
Certitude	minimale ou aucune	moyenne ou raisonnable	élevée

2.2.1 Enjeux modestes, risques faibles

Il s'agit des transactions pour lesquelles il est nécessaire d'avoir une certaine assurance quant à l'identité mais dont les enjeux sont, à tous égards, relativement modestes et les risques faibles. Alors on recherchera une certitude minimale quant à l'identité de la personne.

Dans ces cas, la preuve de l'identité de la personne pouvant procurer une certitude minimale peut être, par exemple, l'affirmation que la personne qui se présente en ligne est bien la personne qu'elle dit être.

L'identification procurant le degré de certitude requis pourra découler simplement de l'affirmation de la personne. Dans les cas qui le nécessitent, on pourra utiliser la possibilité de confirmer l'affirmation par des moyens directs ou indirects.

Il y a d'autres transactions qui ne requièrent pas d'établir son identité, mais où le contact nécessaire à la transaction révèle des informations malgré tout. Cette situation existe tant dans l'environnement physique que dans un environnement électronique comme Internet.

Par exemple :

- Achats au comptant, via un mode de paiement ne nécessitant pas de révéler l'identité – carte à puce de type «portefeuille électronique» etc.
- Demandes d'informations en présence face à face, au téléphone ou par Internet.
- Le fait de se présenter physiquement au comptoir implique la divulgation de ses traits physiques

Mais dans les environnements comme Internet, il est pratiquement impossible de faire une transaction anonyme. L'accès à de l'information publique sur Internet permet, la plupart du temps, d'obtenir des renseignements sur l'usager, que ce soit par le biais des cookies, des variables d'environnement ou de tout autre mécanisme technologique mis à la disposition de l'administrateur de système.

C'est pourquoi lors de transactions ne nécessitant pas d'identifier, il faudra déterminer comment seront traitées les informations dont la transmission pourrait avoir pour conséquence de révéler l'identité du correspondant.

2.2.2 Enjeux sensibles ou importants, risques moyens

Il s'agit ici des transactions requérant une certitude moyenne quant à l'identité de la personne. Les enjeux sont sensibles ou importants, mais demeurent relativement modestes et les risques demeurent moyens.

On vise ici des transactions pour lesquelles il est jugé nécessaire de disposer d'un degré raisonnable de certitude au sujet de l'identité du co-contractant. La preuve de l'identité pourra être plus certaine.

Lors de ces transactions, on peut requérir une identification résultant seulement de l'affirmation du co-contractant ou une identification documentée. On recourt alors à des identifiants fondés sur une information que la personne est la seule à connaître ou encore à la présentation d'un objet qui lui est personnel.

a) L'identification sans le soutien de document

On demande au co-contractant de s'identifier en fournissant des informations qu'il connaît. Dans la majorité des cas, il suffira que les noms, prénoms et adresse soient accompagnés d'une autre information comme la mention du numéro d'assurance sociale, du numéro d'assurance maladie ou des deux (voir en Annexe 1, Tableau 2 - *Exemples d'identification sans le soutien de documents*). Ces documents n'ont pas à être exhibés.

Par exemple, lors de transactions qui s'adressent uniquement aux adultes (achats de boissons alcooliques, de matériels destinés aux adultes), on pourra requérir des informations comme :

- le nom, l'adresse et le numéro de téléphone
- la date de naissance

b) L'identification avec le soutien de documents

Souvent les organismes gouvernementaux exigent une preuve supplémentaire d'identité (voir en Annexe 1, Tableau 3 - *Exemples d'identification avec le soutien de document*). L'individu doit remplir un formulaire et répondre aux questions qui concernent son identité qu'il devra accompagner de documents qui soutiennent ses prétentions.

Les informations requises sont habituellement :

- le nom, l'adresse et le numéro de téléphone;

- parfois, le nom de son père et de sa mère;
- la date de naissance;
- le statut marital.

De plus, il devra fournir les documents requis par la loi attestant cette identité comme :
- un certificat de naissance;
- un passeport; ou
- une attestation de résidence permanente.

c) L'identification accompagnée de formalités

L'identification d'un individu peut, dans certains cas, être plus formelle et nécessiter un niveau de fiabilité supérieure aux exigences décrites plus haut (voir en Annexe 1, Tableau 4 - *Exemples d'identification accompagnée de formalités*).

Il peut être nécessaire, dans ces cas, que la photo fournie par un demandeur soit signée par une autre personne ou que l'assermentation d'une personne soit faite en présence d'un témoin pour s'assurer de l'identité de la personne comme l'exige la *Loi électorale*.

2.2.3 Enjeux très sensibles ou très importants, risques élevés

Pour certaines transactions, le niveau de risque et l'ensemble des enjeux impliqués sont tels qu'ils emportent un besoin très élevé de certitude quant à l'identité de la personne concernée.

Plusieurs de ces transactions sont, en vertu des lois et des règlements, assujetties à des exigences spécifiques visant à préciser le degré de certitude qui doit être alors recherché. Pour certaines, la loi exige que l'on ait recours à un mécanisme faisant en sorte que les informations soient authentiques (a). Il y a d'autres transactions qui impliquent des informations confidentielles (b). Ce sont des cas particuliers de transactions aux enjeux très sensibles ou très importants et comportant des risques élevés.

- Des transactions nécessitent une preuve de l'identité d'une personne :
  - Accès à certains services gouvernementaux (permis de conduire, accès à des dossiers personnels).
  - Transactions de produits financiers (ouverture de compte, transaction d'une somme importante).
  - Transactions avec des organismes gouvernementaux (ministère du Revenu, Aide juridique).

La difficulté dans ce genre de transactions consiste à déterminer quels documents ou quels moyens permettent d'affirmer qu'il s'agit véritablement de la bonne personne. Dans certaines situations, la présentation d'une pièce d'identité sera suffisante (carte d'assurance maladie, permis de conduire). Dans d'autres situations, la signature manuscrite de la personne sera aussi requise aux fins de comparaison.

- Certaines transactions impliquent la divulgation de renseignements personnels particuliers (âge, sexe, numéro d'assurance maladie et numéro d'assurance sociale, renseignements financiers).

La fourniture en ligne de certains services gouvernementaux et de certaines prestations prévues par les lois et règlements est assujettie à diverses conditions et exigences. Parmi ces exigences, il en est qui consistent à exiger de fournir certains renseignements personnels comme le numéro d'assurance sociale, le numéro d'assurance maladie ou le numéro de permis de conduire.

Un organisme peut, par exemple, demander à une personne de s'identifier en inscrivant dans l'espace approprié à cette fin son numéro d'assurance sociale ou de payer par l'intermédiaire de sa carte de crédit en inscrivant son numéro.

- D'autres transactions nécessitent la signature d'une ou des parties. C'est le cas par exemple :
  - des actes sous seing privé. (par exemple, un contrat de vente d'une pièce d'ameublement)
  - de la plupart des documents administratifs (rapports d'impôts, actes de constitution d'entreprise, etc.).

Les actes sous seing privé contiennent obligatoirement la signature des parties sans quoi ils ne peuvent être qualifiés comme tel. Toutefois, il n'est pas toujours nécessaire qu'un acte administratif porte la signature de la personne. La signature constitue uniquement une preuve supplémentaire de la volonté de la personne exprimée dans le document.

- En certaines circonstances, il est nécessaire que l'identification soit attestée par une personne.

Ainsi, la loi impose aux professionnels de la santé d'identifier clairement leurs clients dans les dossiers-clients. À ce titre, ceux-ci ont le devoir de «consigner au dossier les nom, adresse, date de naissance, sexe» et certains autres renseignements plus spécifiques au service offert par un professionnel[13]. Selon le *Règlement sur la tenue des dossiers d'un médecin*, «le médecin doit insérer au dossier médical qu'il a constitué les renseignements, les observations et les *documents suffisants pour décrire clairement l'identité du patient*»[14].

D'autre part, afin d'aider la recherche et la poursuite d'infractions reliées au recyclage des produits de la criminalité, différents établissements tels les banques, les caisses populaires, les sociétés d'assurance-vie, les casinos etc, ont l'obligation de s'assurer de l'identité de

---

13 Voir par exemple : *Règlement sur la tenue des dossiers et des bureaux d'affaires des podiatres,* R.R.Q. (1981), P-12 art. 2.02; *Règlement sur la tenue des dossiers, livres et registres par un pharmacien dans l'exercice de sa profession*, R.R.Q. (1981), P-10, r.11, art.2.02; *Règlement sur la tenue des dossiers et le maintien d'équipement d'un dentiste*, (1993) 125 G.O.II, 5887, art. 3.

14 *Règlement sur la tenue des dossiers d'un médecin,* (1992) 124 G.O.II 3090, art. 2.2.

chaque individu qui signe la fiche de spécimen de signature d'un compte ouvert auprès d'elles[15]. Par ailleurs, la loi oblige les institutions, pour tout dépôt de 10 000$ ou plus en espèces, de tenir et conserver un relevé d'opérations importantes, et inscrire le nom et l'adresse de l'individu remettant ce montant.

- Dans certaines circonstances, la loi exige que l'identification soit faite par des officiers publics (voir en Annexe 1, Tableau 5 - *Exemples d'identification attestée par un officier public*).

Par exemple, le notaire a l'obligation de «vérifier l'identité des parties dont il reçoit la signature par tout moyen raisonnable lui permettant d'établir cette identité» *(Loi sur le notariat*, L.R.Q., c. N-2, art. 41). De plus, l'article 40 (1) précise que la présence des parties devant le notaire instrumentant est en principe nécessaire.

Les actes sous seing privé dont on requiert l'inscription au registre foncier doivent être complétés par une attestation faite par un notaire ou un avocat (art. 2991 C.c.Q.). L'auteur de l'attestation devra indiquer qu'il a vérifié l'identité, la qualité, et la capacité des parties à l'acte sous seing privé.

Enfin pour l'inscription sur le registre foncier des déclarations de résidence familiale, des baux immobiliers ou des avis prévus à la loi, l'article 2995 du Code civil indique que «les documents présentés n'ont pas à être attestés par un notaire ou un avocat, mais par deux témoins, dont l'un sous serment». Par ailleurs, l'attestation de vérification présentée par un notaire, un avocat, un arpenteur-géomètre ou un officier public établit une présomption qui exempte l'officier de la publicité des droits de toute vérification supplémentaire (art. 3009 C.c.Q.).

a) Les transactions nécessitant l'authenticité de l'information

Certaines transactions ne peuvent être conclues qu'à la condition que les informations qui leur sont inhérentes soient authentiques.

Par exemple,

- Documents ou actes administratifs.
- Documents qui émanent d'une autorité publique.
- Rapports d'experts ou d'enquêtes.
- Documents qui nécessitent une publication au bureau de la publicité des droits.
- Certains actes notariés.
- Les procès verbaux de bornage, etc.

---

15 Article 11 a) du *Règlement sur le recyclage des produits de la criminalité,* (1993) 127 Gaz. Can. II 1009. Les alinéas b) à f) obligent l'identification en certaines autres circonstances comme lors d'opérations de change, de commerce de valeurs mobilières, de transactions avec des compagnies d'assurance-vie ou avec des casinos.

Le caractère authentique de ces documents suppose un degré très élevé de fiabilité. Dans certains cas, il est essentiel que non seulement l'identité des parties soit vérifiée mais aussi leur qualité et leur capacité.

Dans le monde physique, ces différents documents émanent d'officiers ministériels, d'experts, d'avocats, de notaires ou d'arpenteurs-géomètres. Les documents qui nécessitent une publication exigent, la plupart du temps, que l'identité, la qualité et la capacité des parties soient vérifiées et attestées par un avocat ou un notaire. Les actes notariés et les procès-verbaux de bornage sont les documents les plus difficiles à répudier en raison des formalités strictes auxquelles ils sont assujettis.

Ainsi, il est important de s'assurer, avant même la signature du document, que les personnes signataires ont l'autorité nécessaire et la capacité requise pour apposer leurs signatures.

Dans le monde virtuel, on peut penser que dans ces cas, il sera nécessaire de recourir à des agents certificateurs de l'identité dont la fonction est de certifier l'identité des détenteurs de certificats numériques d'identité ou de clés cryptographiques et l'authenticité du document électronique.

b) Les transactions impliquant des informations confidentielles

Plusieurs transactions supposent l'échange d'informations qui sont confidentielles. L'identification adéquate devient alors un enjeu très important car en raison de la nature de pareils documents, il est exclu qu'ils soient transmis à la mauvaise personne ou à une personne qui n'y a pas droit. À titre d'exemple, on peut mentionner les catégories suivantes d'informations :

- Courrier confidentiel.
- Documents à portée contractuelle.
- Dossiers d'employés.
- Dossiers personnels (impôts et revenu, santé, etc.).
- Information stratégique.
- Paiements.
- Plaintes.
- Rapports d'experts ou d'enquêtes, etc.

Dans le monde physique, la transmission d'informations confidentielles peut prendre différentes formes. Du simple chuchotement à l'oreille d'une personne en particulier, à l'envoi d'un courrier recommandé portant la mention "strictement confidentiel". Pour avoir accès à de l'information confidentielle, il faut, la plupart du temps, posséder une clé ou se voir attribuer un droit d'accès en raison de son poste ou de sa fonction. Ainsi, seulement la ou les personnes autorisées pourront accéder à ces informations. Par ailleurs, le droit au secret professionnel, contenu dans plusieurs lois et attribué à diverses personnes en raison du caractère confidentiel des informations divulguées à certains professionnels, accroît le nombre de situations qui exigent que la confidentialité des informations soit préservée.

Dans le monde virtuel, la difficulté provient du fait que l'information transmise peut être détournée à tout moment. C'est pourquoi, il faut prévoir des mécanismes qui garantiront la confidentialité des données transmises. De plus, il est important que ces informations soient assurées du même degré de confidentialité lors de leur conservation. Les outils de chiffrement des données permettent de garantir la confidentialité des informations et de s'assurer que l'accès à celles-ci soit réservé uniquement aux personnes autorisées.

2.2.4 Les risques et les responsabilités en matière d'identification

Le tableau qui suit illustre la variété de situations transactionnelles qui peuvent survenir dans la vie courante d'une personne et identifie les risques et les responsabilités de chacune de ces catégories de transaction.

Types de transaction	**Risques et responsabilités en matière d'identification**	
	Monde physique	**Monde virtuel**
1. Les transactions anonymes ➢ Achats au comptant ➢ Demandes d'informations	Peu de risques donc peu de responsabilités en matière d'identification.	Identification des composantes de l'environnement de l'ordinateur de l'usager. Risques d'atteinte à la vie privée si les données recueillies sont regroupées.
2. Les transactions qui impliquent la divulgation de renseignements généraux (nom, adresse et numéro de téléphone) ➢ Transactions par téléphone ➢ Accès à certains services	Peu de risques donc peu de responsabilités en matière d'identification	Identification des composantes de l'environnement de l'ordinateur de l'usager. Risques d'atteinte à la vie privée si les données recueillies sont regroupées.
3. Les transactions qui impliquent la divulgation de renseignements personnels particuliers ➢ Achats (utilisation de la carte de crédit ou de la carte de débit) ➢ Transactions avec des organismes gouvernementaux ➢ Accès à certains services	Renseignements reliés directement à la personne. Obligation pour la partie qui recueille les renseignements de respecter les lois relatives à la protection des renseignements personnels.	La divulgation de renseignements en ligne reliés directement à la personne engendre des risques de détournement des données, d'usurpations d'identités et d'atteintes à la vie privée. Obligation pour la partie qui recueille les renseignements de respecter les lois relatives à la protection des renseignements personnels.
4. Les transactions qui nécessitent une preuve de l'identité d'une personne - Transactions qui s'adressent uniquement aux adultes - Accès à certains services gouvernementaux - Transactions de produits financiers	Le fait de ne pas s'assurer de l'identité de la personne peut entraîner la responsabilité de la partie qui avait cette obligation.	Le fait de ne pas s'assurer de l'identité de la personne peut entraîner la responsabilité de la partie qui avait cette obligation.
5. Les transactions qui nécessitent la signature d'une ou des parties ➢ Les actes sous seing privé ➢ Documents administratifs	L'absence de signature constitue un défaut qui peut affecter la validité de l'acte.	L'absence de signature constitue un défaut qui peut affecter la validité de l'acte.

Types de transaction	Risques et responsabilités en matière d'identification	
	Monde physique	**Monde virtuel**
6. Les transactions qui nécessitent l'authenticité de l'information ➢ Documents ou actes administratifs ➢ Documents qui émanent d'une autorité publique ➢ Rapports d'experts ou d'enquêtes ➢ Documents qui nécessitent une publication au bureau de la publicité des droits ➢ Actes notariés ➢ Procès-verbaux de bornage	Le caractère authentique exige un degré très élevé de fiabilité du contenu. Dans certains cas, non seulement l'identité des parties doit être vérifiée, mais également la qualité et la capacité. Il s'agit généralement de documents qui émanent d'une entité gouvernementale ou de professionnels qui sont habilités à recevoir ce genre d'actes. Ceux-ci engageront leurs responsabilités en cas d'erreur.	Le caractère authentique exige un degré très élevé de fiabilité du contenu. Dans certains cas, non seulement l'identité des parties doit être vérifiée mais également la qualité et la capacité. Il s'agit généralement de documents qui émanent d'une entité gouvernementale ou d'un professionnel. Des agents certificateurs de l'identité doivent être spécifiquement désignés dont la fonction sera de certifier l'identité (qualité et capacité) des détenteurs de clés et l'authenticité des documents électroniques. Ceux-ci engageront leurs responsabilités en cas d'erreur.
7. Transactions qui nécessitent que la confidentialité des informations soit préservée ➢ Courrier confidentiel ➢ Document à portée confidentielle ➢ Données confidentielles ➢ Dossiers d'employés ➢ Échange d'informations ➢ Dossiers personnels ➢ Information stratégique	L'identification de la personne est importante compte tenu du caractère confidentiel et du degré de sensibilité des informations. Le fait de ne pas s'assurer de l'identité de la personne peut entraîner la responsabilité de la partie qui avait cette obligation.	L'identification de la personne est importante compte tenu du caractère confidentiel et du degré de sensibilité des informations. Le fait de ne pas s'assurer de l'identité de la personne peut entraîner la responsabilité de la partie qui avait cette obligation.

Dans le monde physique, les transactions anonymes et les transactions n'impliquant que la divulgation de renseignements généraux (points 1 et 2) n'engendrent que peu de responsabilité en matière d'identification. Compte tenu du caractère impersonnel et anodin de ce genre de transactions, il n'est pas nécessaire de connaître des détails spécifiques sur l'identité des parties. Autrement dit, dans ce genre de transactions, les parties analysent les risques découlant de la non-identification comme étant relativement faibles.

Dans le monde virtuel, aucune transaction, même celles qui sont anodines, n'y est totalement anonyme. La présence de cookies et de variables d'environnement de même que le couplage des données recueillies peuvent permettre d'identifier les individus avec plus ou moins de précision.

Pour ce qui est des transactions qui impliquent la divulgation de renseignements personnels (point 3), la problématique se pose de façon différente. Ces renseignements sont, par leur nature, confidentiels et correspondent à une personne en particulier. Cette situation illustre le fait que l'identification est parfois requise afin d'assurer le maintien du caractère confidentiel de certaines informations. Généralement, la personne qui veut transiger n'a pas la possibilité de refuser de fournir les renseignements personnels. De son côté, l'entité qui recueille les renseignements a des obligations à respecter en vertu des lois sur la protection des renseignements personnels.

Certaines transactions concernent spécifiquement l'identité de l'individu (points 4, 5 et 6). Plusieurs mécanismes sont alors mis en place pour s'assurer de l'identité de la personne. Pièces d'identité, signatures, témoins, attestations, etc. Dans tous ces cas, l'identification de la personne est nécessaire. Plus particulièrement, lorsque la transaction nécessite une preuve de l'identité d'une personne (point 4), il peut être requis de vérifier l'identité de la personne mais aussi la qualité et la capacité des parties.

Enfin, il y a les transactions qui nécessitent la préservation de la confidentialité des informations (voir point 7). La particularité de cette dernière situation est liée au fait qu'indépendamment du type de transaction, la confidentialité requiert que ces informations soient accessibles uniquement aux personnes expressément désignées. L'identification des personnes prend alors une grande importance.

Cette typologie permet de constater que l'identification d'une personne s'opère de manière différenciée lorsqu'elle est nécessaire, soit pour des raisons reliées à la preuve ou pour préserver le caractère confidentiel de l'échange. Les parties vont ressentir des besoins plus élevés de certitude quant à l'identité en fonction des risques impliqués dans la transaction. Dans le monde réel, l'identification peut s'effectuer de différentes façons selon le degré de fiabilité désiré et les risques que l'on est prêt à tolérer. L'absence d'identification préalable peut engendrer des répercussions négatives qui peuvent engager la responsabilité des parties.

Dans le monde virtuel, il paraît plus difficile d'opérer une gradation aussi variée. De plus, la particularité des réseaux ouverts nécessite un degré supérieur de minutie compte tenu des plus fortes possibilités d'usurpation d'identité, d'atteinte à la vie privée et de détournement de renseignements personnels comme, par exemple, le numéro de la carte de crédit. C'est pourquoi on estime souvent que les mécanismes technologiques reliés à la cryptographie et aux signatures numériques doivent être utilisés à partir du moment où l'association d'une personne avec une donnée est nécessaire pour confirmer la validité d'une transaction.

Mais avant de procéder au choix des moyens d'identification, il faut situer les balises au-delà desquelles il n'est pas permis de réclamer des informations aux fins d'identification. C'est l'objet de la troisième étape.

3. Troisième étape : Baliser la collecte et le traitement de l'information personnelle

Dans l'absolu, on peut se prendre à rêver d'un système dans lequel on collecte et collige tous les renseignements permettant d'identifier et de vérifier l'identité d'une personne même pour faire face aux situations exceptionnelles. Mais un équilibre doit être respecté entre une collecte tous azimuts d'information et une approche de protection de la vie privée qui rendrait les transactions trop risquées. Aussi, après avoir établi les besoins d'identification et déterminé le degré requis de certitude, il faut considérer les limites imposées au nom de la protection de la vie privée des personnes.

En tant que processus supposant différents échanges d'information, l'identification présente à la fois des avantages et des écueils. Dans la plupart des situations, il faut mettre en place un environnement garantissant un équilibre entre les besoins de certitude dans l'identification et la protection des droits de la personne, notamment à la vie privée.

C'est pourquoi les processus d'identification électronique doivent êtres conçus de manière à respecter les principes des lois relatives à la protection des informations personnelles.

L'on s'accorde généralement à reconnaître que le droit à la vie privée suppose un droit de regard sur les informations qui y sont relatives et un droit balisé à l'anonymat. Dans l'univers des transactions électroniques, cela se traduit par un devoir de retenue dans les demandes d'informations personnelles et l'obligation de mettre en place ce qui est nécessaire afin que les personnes puissent en tout temps exercer leur droit de regard sur les informations qui les concernent.

En matière de protection de renseignements personnels, le principe de retenue (limitation en matière de collecte) vient guider les gestionnaires confrontés au défi d'assurer un équilibre entre les besoins de certitude, de sécurité et les obligations d'assurer le respect de la vie privée des personnes. En partant du principe suivant lequel on ne doit recueillir que les informations dont on est en mesure de démontrer la nécessité, compte tenu de la transaction considérée, on s'assure que les informations personnelles ne seront collectées que pour une fin clairement identifiable et limitée.

Un droit de contrôle sur l'information personnelle est reconnu dans la plupart des lois sur la protection des renseignements personnels. Une telle reconnaissance présente un double intérêt : elle permet à l'individu de contrôler l'exactitude des données stockées sur son compte et, naturellement en cas de besoin, de les faire rectifier; elle permet également de faire participer l'ensemble des personnes fichées au contrôle du respect des règles en matière d'informations nominatives.

3.1 La démarche

Comme l'identification implique souvent la collecte et le traitement de renseignements personnels, il importe de s'assurer que l'on respecte les principes les plus universellement admis en matière de protection d'informations relatives à la vie privée. L'identification des

personnes dans l'environnement électronique soulève un grand nombre de préoccupations concernant la protection de la vie privée et la sécurité des transactions (voir annexe 1, Tableau 6 - *Les préoccupations rattachées à l'identification des personnes*).

Plusieurs utilisateurs d'Internet craignent que des informations à caractère personnel soient automatiquement générées, collectées, stockées rapprochées et exploitées à des fins diverses.

Les technologies de l'information permettent de recueillir un nombre croissant de renseignements sur un individu. Le développement du commerce électronique s'accompagnera d'une augmentation du volume et de la diversité des données de caractère personnel communiquées sur les réseaux aux cours d'activités et de transactions électroniques. Les nouvelles méthodes utilisées pour traiter de très grandes quantités de données permettent de créer des profils de consommateurs associant données démographiques, informations financières, pratiques de consommation et détails sur les transactions.

La prise en considération des principes relatifs à la collecte et au traitement des informations personnelles permet de mieux cerner les balises et précautions qui doivent êtres mises en place lors de l'établissement de processus d'identification.

Les avantages résultant de l'identification sont variables en fonction des besoins afférents aux différentes interactions et transactions dans lesquelles on s'engage.

Il est donc nécessaire de trouver un équilibre entre les impératifs de la protection des renseignements personnels, des droits individuels, des intérêts commerciaux, du droit à l'information et de l'obligation de l'État d'assurer une gestion correcte de ses programmes, de se protéger et de protéger les citoyens des menaces à la sécurité publique.

Afin de faciliter la détermination concrète des limites au droit de collecter et de traiter des informations personnelles lors de processus d'identification, on peut avoir recours à une grille d'analyse dans laquelle sont consignées les informations permettant d'associer la quantité et la qualité des informations demandées à chacun des principes fondamentaux en matière de collecte et de gestion de l'information personnelle.

Au TERME DE CETTE ÉTAPE, on sera en mesure d'associer les principes devant être respectés lors de la collecte, du traitement et de la conservation d'informations relatives à l'identité d'une personne en regard des risques et enjeux spécifiques à l'environnement que l'on met en place.

Cette démarche permet de compléter le processus de détermination des informations qui sont considérées comme étant nécessaires à la transaction considérée.

Elle aidera à déterminer les moyens acceptables pour obtenir le degré approprié de certitude à l'égard de l'identité d'une personne tout en assurant la protection de sa vie privée.

3.2 Les principes de gestion à respecter

La législation québécoise sur la protection des renseignements personnels limite le droit d'un organisme public ou d'une entreprise de recueillir des informations personnelles[16]. De telles informations ne peuvent être recueillies qu'auprès de la personne concernée ou d'un tiers, en certaines circonstances spécifiques (Loi sur l'accès, art. 65 et Loi sur le secteur privé, art. 6). Les limites au droit de collecter et de traiter des informations personnelles peuvent être synthétisées dans les principes de gestion ci-après explicités.

3.2.1 La nécessité de la collecte d'informations identifiantes

Il faut être en mesure de démontrer la nécessité des renseignements demandés.

Dans le secteur public, il est licite de recueillir un renseignement personnel seulement si cela est nécessaire à l'exercice des attributions de l'organisme public ou à la mise en œuvre d'un programme dont on a la gestion (Loi sur l'accès, art 64).

En vertu de la loi sur le secteur privé, l'on ne peut exiger des informations personnelles autres que celles qui sont strictement nécessaires à la prestation du service proposé ou à l'exécution du contrat. Par exemple, la Commission d'accès à l'information a expliqué, dans sa décision *Bellerose c. Université de Montréal*[17] que par informations nécessaires, il fallait entendre celles qui sont requises, indispensables, obligatoires pour le fonctionnement efficace du service concerné.

C'est à l'organisme ou à l'entreprise qui requiert le renseignement d'établir que ce dernier est nécessaire. Il est donc essentiel, dès la conception d'un système de transaction en ligne, de spécifier avec précision pourquoi chacune des informations personnelles demandées est nécessaire.

La nécessité s'apprécie évidemment en fonction de l'activité et du service concerné. Elle découle non seulement des exigences intrinsèques à la transaction prise isolément mais de l'ensemble du contexte dans lequel s'inscrit l'activité. Ainsi, dans sa décision *Bellerose c. Université de Montréal*, la Commission d'accès conclut que le numéro de téléphone résidentiel était, dans le contexte technique, budgétaire et contractuel de l'organisme public, un renseignement requis pour assurer la fourniture du service.

En vertu de ce principe, seules les informations nécessaires doivent être exigées, recueillies et traitées. La nécessité s'apprécie évidemment en fonction du contexte et des fins pour lesquelles l'information est recueillie.

---

16 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, ci-après citée Loi sur l'accès; *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, ci-après citée Loi sur le secteur privé.

17 (1986) C.A.I. 236.

Les finalités en vue desquelles les données à caractère personnel sont utilisées doivent être déterminées au plus tard au moment de leur collecte. Ces finalités devront être spécifiées par celui qui exige des informations personnelles[18]. Elles devront aussi être portées à la connaissance de la personne concernée.

Ce principe s'inscrit dans une logique voulant que la personne concernée puisse exercer un droit de contrôle sur les renseignements. Lorsqu'il est informé de la finalité pour laquelle on lui demande de fournir des informations personnelles, l'utilisateur est en mesure de formuler un consentement éclairé pour leur collecte.

Les renseignements personnels ne peuvent être utilisés que pour les fins pour lesquels ils ont été recueillis. Si de nouvelles finalités apparaissent, il faut s'assurer d'obtenir le consentement approprié de l'intéressé avant de faire usage des renseignements personnels.

La divulgation ou la transmission des données aux tiers est possible si cela est nécessaire : à l'exécution du contrat entre les parties, au respect d'une obligation légale imposée par une autorité, à la sauvegarde de l'intérêt vital de la personne, à l'exécution d'une mission d'intérêt public, à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement.

Autrement, les données à caractère personnel ne peuvent pas être divulguées, ni transmises à des tiers qu'avec le consentement de la personne concernée[19] ou lorsqu'une règle de droit le permet[20].

C'est pourquoi il faut en tout temps être en mesure d'indiquer quelles sont les utilisations qui sont faites des informations personnelles demandées et détenues.

3.2.2 La détention limitée dans le temps

Le principe de la retenue vaut également pour la durée pendant laquelle les renseignements personnels sont détenus. Les informations personnelles ne doivent être détenues que dans la mesure où elles sont nécessaires à l'accomplissement de la fin pour laquelle elles ont été recueillies. Ainsi, l'article 73 de la Loi sur l'accès prévoit que les organismes publics ont l'obligation de détruire le renseignement nominatif ou de le traiter conformément à la loi sur les archives lorsque l'objet pour lequel il a été recueilli est accompli. Au-delà de la période où le renseignement est utilisé, ces informations doivent être retirées et archivées de manière à en assurer le caractère confidentiel.

---

18 Loi sur l'accès, art. 65; Loi sur le secteur privé, art. 8.

19 Loi sur le secteur privé, art. 13; art. 37 du C.c.Q.

20 Loi sur le secteur privé, art. 18.

3.2.3 La qualité des données

Il faut s'assurer du maintien de la qualité des données personnelles. Celles-ci doivent être maintenues exactes et à jour de manière à servir aux fins pour lesquelles elles sont recueillies et détenues (Loi sur l'accès, art. 72, voir Loi sur le secteur privé, art. 11). L'article 6)1c) de la *Directive européenne* spécifie que de telles données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ».

La législation québécoise repose sur le même souci. Cela appelle la mise en place d'une gestion rigoureuse des données personnelles au sein de toutes les organisations qui en détiennent. Cette obligation se double d'un devoir d'assurer la sécurité.

3.2.4 Les garanties de sécurité

La législation québécoise exige que soient prises des mesures de sécurité propres à assurer le caractère confidentiel des renseignements[21]. Le caractère raisonnable de ces mesures doit être évalué dans le contexte d'Internet[22]. Les mesures doivent être élaborées en fonction du degré de sensibilité des renseignements.

Ces garanties de sécurité peuvent comprendre :

- des mesures d'ordre matériel. Ex. : verrouillage des portes et cartes d'identification;
- des mesures structurelles. Ex. : les niveaux hiérarchiques en ce qui concerne l'accès aux données;
- des mesures informationnelles. Ex. : le chiffrement et la surveillance des activités inhabituelles susceptibles de présenter un danger et des mesures destinées à y faire face. (le protocole Secure Socket Layer "SSL").

Le concepteur doit se doter de règles de conduite précisant ses devoirs et obligations à l'égard des renseignements personnels. Quant aux employés voici quelques mesures devant être prises :

- un code d'accès et un mot de passe pour accéder aux systèmes;
- l'accès limité en fonction des nécessités administratives;
- la signature d'un protocole de confidentialité;

---

21 Loi sur le secteur privé, art. 10 et 17.

22 L'article 17(1) de la *Directive européenne* précise que : «1. Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Voir également les article 7 et 8 de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.*

- la journalisation des consultations des renseignements personnels.

En plus il est nécessaire que tous les préposés soient adéquatement informés des mesures mises en place[23].

3.2.5 La transparence

L'utilisateur doit être en mesure de déterminer facilement l'existence et la nature des données à caractère personnel et les finalités de leur utilisation[24]. Il faut expliquer de façon claire et simple quel type d'information personnelle est recueillie, dans quel but et expliquer la manière dont cette information est traitée[25]. L'utilisateur ne doit pas être laissé dans un état d'incertitude quant à la politique du site concernant la protection des renseignements personnels. Ainsi le concepteur d'un environnement doit éviter que soient recueillies des informations personnelles sans que les utilisateurs soient informés au préalable de la façon dont ces renseignements seront traités et utilisés.

Dans le secteur public, l'établissement d'un fichier de renseignements nominatifs doit faire l'objet d'une déclaration à la Commission d'accès. Cette déclaration doit comporter les indications suivantes :

1° la désignation du fichier, les types de renseignements qu'il contient, l'usage projeté de ces renseignements et le mode de gestion du fichier;

2° la provenance des renseignements versés au fichier;

3° les catégories de personnes concernées par les renseignements versés au fichier;

4° les catégories de personnes qui auront accès au fichier dans l'exercice de leurs fonctions;

5° les mesures de sécurité prises au sein de l'organisme pour assurer le caractère confidentiel des renseignements nominatifs et leur utilisation suivant les fins pour lesquelles ils ont été recueillis;

6° le titre, l'adresse et le numéro de téléphone de la personne responsable de la protection des renseignements personnels;

---

23 Voir CAI, *L'accès à l'information et la confidentialité des renseignements personnels sur l'autoroute de l'information*, septembre 1995, http://www.cai.gouv.qc.ca/auto.htm et OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, 1980.

24 Loi sur le secteur privé, art. 8 et 27; Loi sur l'accès, art. 65 et 83.

25 The Australian Privacy Commissioner's Website, "Guidelines for Federal and ACT Government World Wide Websites", http://www.privacy.gov.au/issues/p7_2.html, page 1 de 4.

7° les modalités d'accès offertes à la personne concernée;

8° toute autre indication prescrite par règlement du gouvernement.

La déclaration doit être faite conformément aux règles établies par la Commission d'accès à l'information.

3.2.6 La responsabilité

Celui qui procède ou fait procéder au traitement des données à caractère personnel assume la responsabilité qui en découle. Il lui incombe de prendre toutes les mesures requises afin que les principes relatifs à la protection des renseignements personnels aient plein effet.

3.2.7 La participation individuelle

Ce principe fait écho au droit de la personne concernée de s'informer de l'existence d'un dossier la concernant et de modifier ou effacer les informations erronées.

Ainsi, la personne a un droit d'accès à son dossier[26], ce qui emporte l'obligation de permettre l'accès à ce dossier d'une manière simple et facile. Le plus souvent, on cherchera à assurer les accès à ces dossiers par un mécanisme en ligne.

En outre, la personne concernée doit avoir la possibilité de corriger ou effacer les informations erronées ou incomplètes la concernant[27]. Elle dispose d'un droit de recours lorsque ces droits lui sont refusés[28].

3.3 Les devoirs et obligations relatifs au traitement et à l'utilisation de l'information identifiante

Au Québec, la loi[29] consacre le caractère confidentiel des renseignements personnels. Ainsi il est prévu un ensemble de mesures visant à encadrer la cueillette de renseignements personnels, leur utilisation, leur conservation et leur communication. Quant à son application, tous les renseignements qui concernent une personne physique et permettent de l'identifier sont visés.

---

26 Voir les articles 38 à 40 du C.c.Q; Loi sur le secteur privé, art. 27 et ss.; Loi sur l'accès, art. 83 et ss.

27 Ce principe a inspiré l'article 12 de la *Directive européenne*. Loi sur l'accès, art. 89 et ss.; Loi sur le secteur privé, art. 28; art. 40 C.c.Q.

28 Loi sur le secteur privé, art. 42 à 53; Loi sur l'accès, art. 135 et ss.

29 Loi sur le secteur privé, art. 10; Loi sur l'accès, art. 53; voir aussi le *Code civil du Québec,* articles 35 à 41.

3.3.1 La démonstration de la nécessité de la cueillette

En règle générale, il faut justifier d'un «intérêt sérieux et légitime» pour recueillir des renseignements personnels.[30] L'organisme public doit être en mesure de démontrer la nécessité d'un renseignement personnel, compte tenu de ses attributions ou d'un programme dont il assure la gestion[31]. Dans la mesure où la personne concernée y consent; la Loi ne fait que formuler les critères suivant lesquels la personne concernée doit être informée des modalités suivant lesquelles une autre personne peut recueillir ou utiliser des renseignements la concernant[32]. En effet, la loi établit une série de critères et d'exceptions concernant la collecte, la détention, l'utilisation et la non-communication des renseignements personnels. Ainsi, la personne constituant un dossier sur autrui doit, lorsqu'elle constitue le dossier, inscrire son objet et ne recueillir, par des moyens licites, que les renseignements nécessaires à l'objet du dossier[33]. Dans le secteur public, les seuls renseignements pouvant être recueillis sont ceux qui ont un lien de connexité avec les attributions de l'organisme ou du programme pertinent.

3.3.2 Le traitement

Une fois les données personnelles collectées d'autres obligations sont imposées par les lois :

- la personne qui détient des renseignements sur une autre personne doit prendre et appliquer des mesures de sécurité pour garantir leur confidentialité[34]
- des mesures doivent être prises pour que les renseignements collectés soient à jour et exacts[35]
- la personne concernée doit avoir la possibilité d'accéder à son dossier[36]
- la personne concernée doit avoir la possibilité de rectifier les renseignements inexacts ou incomplets la concernant[37]
- certaines restrictions à l'accès peuvent être imposées[38].
- les différends quant au traitement des renseignements personnels doivent être soumis à la Commission d'accès à l'information suivant la procédure établie par la Loi[39].

---

30 C.c.Q., art. 37 et la Loi sur le secteur privé, art. 4.

31 Loi sur l'accès, art. 64.

32 L'art. 9 de la Loi sur le secteur privé indique toutefois les circonstances où un individu ne peut pas refuser de fournir un renseignement personnel. Ce sont les cas où la collecte est nécessaire à la conclusion ou à l'exécution d'un contrat, la collecte est autorisée par la loi ou s'il y a des motifs raisonnables de croire que la demande de biens, de services ou d'emploi de l'individu désirant conserver son anonymat n'est pas licite.

33 Loi sur le secteur privé, art. 4 et 5.

34 Loi sur le secteur privé, art. 10; Loi sur l'accès, art. 76.

35 Loi sur le secteur privé, art. 11; Loi sur l'accès, art 72.

36 Loi sur le secteur privé, art. 27; Loi sur l'accès, art 83.

37 Loi sur le secteur privé, art. 29; Loi sur l'accès, art 89.

38 Loi sur le secteur privé, art. 37 à 41; Loi sur l'accès, art. 86 à 88.1.

3.3.3 L'utilisation et la communication des renseignements personnels

Quant à l'utilisation et la communication des renseignements personnels, il importe de s'assurer que :

- l'utilisation des renseignements est interdite lorsque leur objet initial a été accompli[40];
- la communication des renseignements personnels à des tiers est interdite sauf avec le consentement de la personne concernée ou si la loi le prévoit[41];
- un renseignement personnel n'est accessible à un mandataire ou agent de celle-ci sans le consentement de la personne concernée que si ce renseignement est nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat[42];
- une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel contenu dans un dossier qu'elle détient sur autrui dans certaines circonstances prévues par la loi [43]. L'organisme public a aussi cette possibilité mais lorsque cela est nécessaire à l'application d'une loi[44].

Type d'opération	Obligations découlant de la Loi sur le secteur privé	Obligations découlant de la Loi sur l'accès

La cueillette des renseignements personnels	➢ la personne doit avoir un «intérêt sérieux et légitime» pour recueillir des renseignements personnels
	➢ il est nécessaire que la personne concernée consente à cette collecte d'informations.
	➢ la personne constituant un dossier sur autrui doit, lorsqu'elle constitue le dossier, inscrire son objet
	➢ la personne constituant un dossier sur autrui doit recueillir les renseignements personnels par des moyens licites
	➢ seulement les renseignements nécessaires à l'objet du dossier peuvent être collectés
	➢ une personne peut recueillir les renseignements personnels auprès d'un tiers si elle a un intérêt sérieux et légitime et si les renseignements sont recueillis dans l'intérêt de la personne concernée et ils ne peuvent être recueillis auprès de celle-ci en temps
		- L'organisme ne peut recueillir des renseignements nominatifs que si cela est nécessaire à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion.
		- L'organisme qui recueille un renseignement nominatif auprès de la personne concernée doit s'identifier
		- Il doit informer la personne :
		  - du nom, de l'adresse de l'organisme public;
		  - de l'usage auquel ce renseignement est destiné;
		  - des catégories de personnes qui auront accès au renseignement;
		  - du caractère obligatoire ou facultatif de la demande;
		  - des conséquences pour la personne concernée ou du tiers, du refus de répondre à la demande;
		  - des droits d'accès et de

39 Loi sur le secteur privé, art. 42 à 69; Loi sur l'accès, art 135.

40 Loi sur le secteur privé, art. 12; Loi sur l'accès, art. 73.

41 Loi sur le secteur privé, art. 13; Loi sur l'accès, art 59.

42 Loi sur le secteur privé, art. 20.

43 Loi sur le secteur privé, art. 18.

44 Loi sur l'accès, art. 59 et 67.

Type d'opération	Obligations découlant de la Loi sur le secteur privé	Obligations découlant de la Loi sur l'accès
	opportun ➢ une personne peut recueillir les renseignements personnels auprès d'un tiers si elle a un intérêt sérieux et légitime et si la cueillette auprès d'un tiers est nécessaire pour s'assurer de l'exactitude des renseignements ➢ la personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer : de l'objet du dossier; de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise; de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification	rectification prévus à la loi. - L'organisme peut recueillir des renseignements personels auprès d'un organisme privé après en avoir informé la CAI. - Un organisme peut communiquer un renseignement nominatif à toute personne si cela est nécessaire à l'application de la loi. - L'organisme public doit inscrire à un registre toute communication de renseignements nominatifs.
Le traitement des renseignements personnels	➢ la personne qui détient des renseignements sur une autre personne doit prendre et appliquer des mesures de sécurité pour garantir leur confidentialité ➢ des mesures doivent être prises pour que les renseignements collectés soient à jour et exacts pour la prise de décision ➢ la personne concernée doit avoir la possibilité d'accéder à son dossier ➢ la personne concernée doit avoir la possibilité de rectifier les renseignements inexacts ou incomplets la concernant ➢ par ailleurs des restrictions quant à l'accès peuvent être imposées ➢ les différends quant au traitement des renseignements personnels doivent être soumis à la Commission d'accès à l'information suivant la procédure établie par la Loi.	Un organisme public doit veiller à ce que les renseignements nominatifs qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis. L'établissement d'un fichier fait l'objet d'une déclaration à la CAI.. Cette déclaration doit préciser : 1° la désignation du fichier, les types de renseignements qu'il contient, l'usage projeté de ces renseignements et le mode de gestion du fichier; 2° la provenance des renseignements versés au fichier; 3°les catégories de personnes concernées par les renseignements versés au fichier; 4° les catégories de personnes qui auront accès au fichier dans l'exercice de leurs fonctions; 5° les mesures de sécurité prises au sein de l'organisme pour assurer le caractère confidentiel des renseignements nominatifs et leur utilisation suivant les fins pour lesquelles ils ont été recueillis; 6° le titre, l'adresse et le numéro de téléphone de la personne responsable de la protection des renseignements personnels; 7° les modalités d'accès offertes à la personne concernée; 8° toute autre indication prescrite par règlement du gouvernement.

Type d'opération	Obligations découlant de la Loi sur le secteur privé	Obligations découlant de la Loi sur l'accès
L'utilisation et la communication des renseignements personnels	➢ l'utilisation des renseignements lorsque leur objet initial a été accompli est interdite, ➢ la communication des renseignements personnels à des tiers est interdite sauf avec le consentement de la personne concernée ➢ dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible à un mandataire ou agent de celle-ci sans le consentement de la personne concernée que si ce renseignement est nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat ➢ une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel contenu dans un dossier qu'elle détient sur autrui : à son procureur ou au procureur général, lors de la poursuite pour une infraction; à une personne ou à un organisme ayant pouvoir de contraindre à leur communication et qui les requiert dans l'exercice de ses fonctions; à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;.	Lorsque son objet est accompli, le renseignement doit être archivé conformément à la loi ou détruit.

Les principes de gestion de l'information personnelle doivent être connus des usagers. L'entreprise ou l'organisme peut mettre en place une politique de la vie privée (Privacy Policy) dans laquelle le public est informé des pratiques du site quant à l'identification des usagers, au traitement des renseignements personnels ainsi que des mesures de protection prises à l'égard de ces informations. Également, le public doit être informé des mécanismes d'identification automatique, tels les cookies ou les variables d'environnement.

4. Quatrième étape : Déterminer les mécanismes et processus d'identification

Dans la première étape, on a établi pourquoi il faut identifier, dans la seconde étape, on a déterminé le degré de certitude requis quant à l'identification et dans la troisième étape, on a posé les balises qui doivent être respectées lorsqu'on collecte et traite des informations personnelles. Ici, lors de la quatrième étape, il faut déterminer les mécanismes et processus d'identification.

Les mécanismes et processus d'identification permettent d'obtenir le niveau recherché de certitude quant aux qualités d'une personne. Ils sont presque toujours fondés sur le recours et la comparaison de différentes informations.

On regroupe habituellement les mécanismes et processus d'identification en cinq principales approches : ce que l'usager connaît, ce que l'usager possède, ce que l'usager est, le temps et le lieu où se trouve l'usager et le recours à un tiers.

Dans le monde physique, on identifie une personne en lui demandant d'exhiber un objet qu'elle possède comme une carte d'identité, un passeport etc. Dans le cyberespace, il est pratiquement difficile de compter sur des mécanismes informels d'identification du genre de ceux qui sont consciemment ou non utilisés dans les interactions en face à face.

Dans les environnements électroniques, l'identification se fait habituellement en établissant un lien entre la personne et un document associé à une interaction. L'identification s'effectue généralement au grâce à un processus d'échange et de vérification d'information. La preuve de l'identité d'une personne peut se faire par différents moyens. Des mécanismes peuvent être mis en place afin de s'assurer qu'il s'agit de la bonne personne comme le recours à un mot de passe ou à une carte d'identité électronique. Des outils plus fiables, comme la signature électronique, peuvent aussi être utilisés dans certains cas.

Les environnements de transactions électroniques comme Internet favorisent l'amplification de la fonction d'identification de la signature. Dans les rapports contractuels prenant place dans l'espace physique, le rôle identificateur de la signature est plutôt mineur. La vérification d'identité n'intervient que dans les situations exceptionnelles et a posteriori.

La démarche consiste à rechercher les moyens permettant d'obtenir le degré requis de certitude quant à l'identification. Pour arriver à décider de ce qui est requis, il faut croiser la démarche ici proposée avec les résultats obtenus lors de la DEUXIÈME et la TROISIÈME ÉTAPE.

Nous décrivons donc ici brièvement les différents mécanismes et processus d'identification en présentant les avantages, les inconvénients, les préoccupations ou les obligations reliées à l'utilisation de chacun.

4.1 Les mécanismes et processus d'identification fondés sur l'information obtenue de l'usager

L'identification consiste le plus souvent à se nommer. L'identification peut s'effectuer avec ou sans l'aide de documents d'identification.

4.1.1 Les messages électroniques

La transmission d'une demande d'informations à un site faite par courrier électronique dévoile l'adresse électronique de l'émetteur et naturellement, les autres informations qu'il inscrit de manière volontaire.

Le site assume alors une obligation d'informer l'individu s'il y a collecte et conservation de son adresse électronique.

4.1.2 L'usage du nom

L'usage du nom représente un autre moyen très répandu pour identifier un individu. L'utilisation du nom est d'ailleurs présente dans la plupart des processus d'identification et de vérification d'identité du fait des avantages indéniables que ce moyen présente au chapitre de la simplicité d'utilisation et de l'universalité.

Le nom permet principalement de retracer une personne ou son dossier. Par ailleurs, le nom ne permet pas de s'assurer de la vraie identité de la personne. En effet, le simple fait d'énoncer un nom ne garantit pas qu'on est la personne portant tel nom. Il est donc nécessaire d'utiliser un moyen d'identification additionnel, tel un mot de passe ou un numéro d'identification personnelle (NIP).

On peut utiliser le nom comme seule méthode d'identification pour des réservations (à l'hôtel, au restaurant), l'enregistrement d'un logiciel en ligne ou la commande de produits (par exemple, chercher une pizza au comptoir). Pour toutes ces transactions, il importe peu si l'individu utilise une fausse identité ou un faux nom puisque le nom dans ces transactions n'est utilisé que pour le repérage de la personne.

Avantages

- un certain niveau de fiabilité si associé à des mots de passe
- facilité d'utilisation
- coût minime
- utilisé essentiellement à des fins de repérage

Inconvénients

- fiabilité parfois déficiente

4.1.3 Les formulaires

Plusieurs sites web collectent des informations à travers différents formulaires (inscriptions, enquêtes, commentaires, paiement). On distingue :

- les informations obligatoires correspondant aux données d'identification et de paiement indispensables pour s'abonner ou réaliser une transaction
- les informations nécessaires pour la fourniture des biens et des services
- les informations facultatives servant surtout à créer des profils d'usagers, établir des statistiques etc.

Face aux renseignements fournis par l'individu dans les formulaires, plusieurs obligations incombent au site :

- les informations facultatives doivent être clairement séparées des informations obligatoires et regroupées dans un bloc distinct.
- le site doit avoir une politique explicite et accessible à l'égard des données sensibles collectées. Ainsi, il doit s'engager à respecter le degré de confidentialité et de sécurité que commandent les informations collectées et transmises.
- tout site qui collecte des données personnelles doit offrir aux usagers la possibilité de s'opposer à cette collecte. Cette possibilité d'opposition doit s'exercer plus particulièrement à l'égard des traitements commerciaux, aux extractions de listes destinées à des tiers et aux croisements de listes qui peuvent éventuellement être effectués. L'opposition doit pouvoir également s'exercer à l'égard des agences de publicité qui réalisent des ciblages.

4.2 Les mécanismes et processus d'identification fondés sur ce que l'usager connaît

Dans les méthodes et processus d'identification fondés sur ce que l'usager connaît, on vérifie une information que connaît une personne. Pour plus de sécurité, on privilégie le recours à une information qu'elle seule est supposée connaître.

4.2.1 Le code secret

Plusieurs systèmes de transactions reposent sur des codes secrets afin d'identifier des individus comme les codes d'accès (login) et les NIP (numéros d'identification personnels) bancaires. Actuellement, les institutions financières font largement appel à l'utilisation de numéro d'identification personnel assigné au porteur dans le cadre des services liés aux cartes de paiement. La majorité des contrats signés entre les institutions financières et les porteurs de cartes oblige ces derniers à tenir secret leur NIP. La nécessité pour le porteur de la carte à mémoire de garder secret son code d'identification personnel apparaît d'autant plus importante si les clauses de signature implicite demeurent dans les contrats conclus entre les institutions financières et les porteurs de cartes[45]. Actuellement, ces clauses de

45 Voir, par exemple, l'article 3 de la «Convention d'utilisation du guichet automatique» des Caisses populaires et d'économie Desjardins et l'article 1 de l'«Entente relative à l'utilisation des services bancaires automatisés» de la Banque Nationale du Canada.

signature implicite confèrent à l'usage simultané de la carte et du NIP la même valeur que la signature manuscrite du titulaire de la carte.

Avantages
- facilité d'utilisation
- coûts minimes
- un niveau de fiabilité élevé lorsqu'associé, par exemple, à une carte à microprocesseur

Inconvénients
- Plusieurs problèmes au plan de la gestion et de la sécurité : oubli, confusion, dévoilement involontaire
- Lorsque le code est inscrit et transmis en clair, possibilité d'interception et d'utilisation non autorisées; Dans les transactions en ligne, le risque d'interception de ces codes secrets est accru en raison du niveau peu sécuritaire du réseau Internet.
- la possibilité de retracer des mots de passe
- le dévoilement involontaire d'un mot de passe par oubli de quitter ou sortir d'un programme ou site web.

4.2.2 Le numéro d'identification

Les numéros d'identification tels les numéros d'assurance sociale, d'assurance maladie ou de permis de conduire sont aussi utilisés afin d'identifier une personne.

Les numéros d'identification sont généralement émis par des organismes publics afin de simplifier la gestion d'un grand nombre de dossiers administratifs.

Ils sont généralement associés à une carte (jetons physiques).

En pratique, ces numéros sont souvent utilisés à des fins d'identification par une autre organisation que l'organisme émetteur.

Avantages
- efficacité pour l'indexation des dossiers et leur repérage.

Inconvénients
- lacunes au plan de la sécurité. La quantité importante de fraudes qui existent au niveau des numéros et cartes d'assurance sociale au Canada en est un exemple.
- Même si en pratique, certains numéros sont généralement utilisés, les règlements encadrant leur utilisation comportent des interdictions de les exiger à des fins d'identification étrangères aux programmes pour lesquels ils sont émis
- délais pour l'émission ou le renouvellement d'une carte
- niveau de fiabilité variable
- risques liés à la constitution de banques de données conservant ces numéros d'identification

4.3 Les mécanismes et processus d'identification fondés sur ce que l'usager possède

Dans le monde physique, l'on s'identifie parfois en apposant notre signature. Quelquefois, l'identification consiste à exhiber une carte qui atteste notre appartenance à un groupe ou à un organisme (Ex : lors de la location d'un livre à la bibliothèque ou d'un film dans un club vidéo). Ce que l'on possède peut en effet servir à nous identifier avec un bon degré de certitude.

4.3.1 Les jetons physiques

Le recours à des jetons physiques est également un moyen très répandu afin de vérifier l'identité d'une personne. La carte de plastique représente l'une des formes de jetons physiques que l'on qualifie de jeton passif.

On distingue les jetons passifs et actifs

Les jetons passifs prennent généralement la forme d'une carte informatique pourvue d'une surface magnétisable sur laquelle sont stockées des données par enregistrement magnétique.

Simple dépôt d'informations, la carte magnétique ne peut procéder à des opérations logiques ni effectuer le moindre traitement. Par exemple, si elle est couplée à un numéro d'identification personnel (NIP), c'est un dispositif interne de l'appareil lecteur qui possède l'algorithme de vérification de celui-ci et non la carte elle-même.

Les jetons passifs peuvent donner lieu à la contrefaçon. Le jeton passif est généralement associé à différents autres moyens d'identification et de vérification d'identité tel un numéro, le nom, la signature ou la photographie.

Pour des raisons pratiques (notamment la nécessité d'une interface capable de lire le jeton) et de sécurité, le jeton passif peut rarement être utilisé à distance et suppose généralement la présence physique du détenteur.

Il y a enfin les jetons dits actifs; la carte à microprocesseur en est un exemple.

4.3.2 Les cartes à microprocesseur

Plusieurs appellations sont utilisées pour désigner les cartes comportant des circuits électroniques : on parle de carte à mémoire, de carte à microcircuit, de carte à puce ou de carte à microprocesseur.

La carte à microprocesseur permet :

- l'authentification de la carte par le terminal dans lequel elle est introduite ou par la centrale à laquelle est relié le terminal;
- l'identification de l'utilisateur avec le détenteur par la comparaison entre le NIP (ou la clé) introduit par celui-ci et celui contenu dans une zone de référence de la carte;
- la certification de l'inscription de certaines données en mémoire sur la carte, assurant ainsi leur intégrité et leur conservation;
- le chiffrement des données, grâce à l'inclusion dans la carte d'un algorithme cryptographique comme le DES, sécurisant les données contre ceux qui n'ont pas accès à la clé;
- la sécurisation d'un réseau : les terminaux qui sont branchés sur le réseau ne peuvent y avoir accès qu'après l'introduction d'une carte valide dans un lecteur approprié et de la clé qui lui est associée.

Avantages

- niveau de sécurité et fiabilité assez élevé (notamment par rapport aux mots de passe)
- permet de faire signer des documents en ligne ou autoriser des transactions d'une manière beaucoup plus fiable
- portabilité : on peut utiliser la carte de n'importe quel poste de travail doté d'une interface appropriée
- possibilité de stockage des données personnelles (un profil) de l'individu sur la carte elle-même
- intégrité et conservation des données personnelles stockées;
- association possible avec le paiement électronique (en effet la carte pourrait constituer à elle seule l'outil pour faire des paiements directs en ligne et aussi pour autoriser les transactions)
- efficacité :la carte accélère la transaction ou l'inscription de l'individu puisque l'identification se fait de façon automatique (surtout au niveau de l'inscription)
- facilite le travail des institutions financières pour l'identification des clients lors de l'ouverture d'un compte ou des opérations de change

Inconvénients

- crainte de surveillance gouvernementale ou policière (surtout dans le cas d'une carte unique multiservice)
- danger de vol ou perte (puisque la carte est un objet extérieur à l'individu, son utilisation doit être assujettie à un mot de passe)

4.3.3 La signature numérique

Dans le monde virtuel, le concept de signature prend une signification passablement différente de celle qui lui est attribuée dans le monde papier puisqu'il permet d'identifier la personne. En effet, le mécanisme de cryptographie à clé publique permet aux détenteurs de la clé d'authentifier leurs documents à l'aide d'une clé privée qui génère une signature numérique[46]. Outre la certitude qu'elle procure quant à l'identité de la personne, cette technique garantit l'intégrité des documents et permet aux destinataires de déterminer si un message a été modifié pendant sa transmission.

Les procédés de signature à clés publiques, ou encore de signature numérique, sont de plus en plus utilisés dans le commerce électronique.

Dans un système à clé publique, la réalisation des différentes fonctions d'identification suppose qu'une personne dispose de deux clés mathématiques complémentaires : une clé privée, dont le caractère secret doit effectivement être préservé, et une clé publique, qui peut être librement distribuée.

46 Consulter le site de Entrust, www.entrust.com, American Bar Association, Section of Science and Technology, «Digital Signature Guidelines Tutorial», http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html, «Terminologie d'Internet», http://www.olf.gouv.qc.ca/ressources/internet/fiches/8384641.htm, Centre de la sécurité des télécommunications, «Qu'est-ce qu'une signature numérique?», http://www.cse-cst.gc.ca/cse/francais/gov4.html. Notarius, «Qu'est-ce que la signature numérique?», http://icp.notarius.com/not2.htm; Charles CÔTÉ, «Bientôt votre signature sur vos documents électroniques», *La Presse*, 15 mai 2000, B1; TRUDEL, P., G. LEFEBVRE et S. PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Publications du Québec, Direction générale des technologies de l'information, ministère des Communications du Québec, 1993.

En annexe 2, sont décrites deux techniques de signature numérique, soit la signature fondée sur la cryptographie asymétrique (RSA) et celle basée sur le Digital Signature Standard (DSS).

Avantages

- niveau de sécurité élevé (le niveau de sécurité dépend toutefois des technologies employées, comme RSA, DSS)
- possibilité de faire identifier la provenance d'un message ou d'un document par l'appui de la signature électronique
- un des seuls moyens pour faire authentifier un message ou document.

Inconvénients

- le dysfonctionnement du réseau de communication
- l'usurpation d'identité (la mascarade) (lorsque la confidentialité de la clé privée est compromise, celle-ci peut être frauduleusement utilisée par un tiers pour signer différents messages sans qu'il soit possible au destinataire de déceler cette fraude)
- la modification des données après l'apposition de la signature
- la répudiation par l'émetteur du message (dans le cas d'une erreur, un acte de piratage ou un simple refus)
- l'incertitude quant à la valeur juridique de la signature numérique, notamment quant à son admissibilité en preuve[47].

4.4 Les mécanismes et processus d'identification fondés sur ce que l'usager est - les données biométriques

Il s'agit ici des méthodes d'identification fondées sur la comparaison entre les caractéristiques d'une personne et celles qui sont présentées lors d'une transaction.

Les traits de la personne peuvent être utilisés dans le cadre de processus d'identification fondés sur la physiologie naturelle d'une personne. On parle alors d'identification biométrique.

La biométrie s'appuie sur la prise en compte d'éléments morphologiques uniques et propres des individus, tels que les caractères physiologiques ou les traits comportementaux automatiquement reconnaissables et vérifiables[48]. Certaines techniques biométriques sont décrites à l'annexe 3.

47 Voir la *Loi sur la protection des renseignements personnels et les documents électroniques*, 2000, ch.5 (sanctionnée le 13 avril 2000). L'article 31(1) définit la «signature électronique» comme «[s]ignature constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres symboles sous forme numérique incorporée, jointe ou associée à un document électronique». L'article 43 précise que : «Sous réserve des articles 44 à 46, dans le cas où une disposition d'un texte législatif exige une signature, la signature électronique satisfait à l'obligation si les conditions suivantes sont réunies : a) la disposition ou le texte législatif est inscrit sur la liste figurant à l'annexe 2 ou 3; b) les règlements visant l'application du présent article à la disposition ont été observés.».

48 Pour plus d'informations sur la biométrie consulter : Biométrie Online, http://biometrie.online.fr; dmoz, http://dmoz.org/Computers/Security/Biometrics; AVANTI, http://www.biometric.freeserve.co.uk; afb, http://www.afb.org.uk; IBIA, http://www.ibia.org; Biometric Identification, http://www.biometricid.com.

Ainsi il existe deux catégories de technologies biométriques :

1. Les techniques d'analyse du comportement :
   - la dynamique de la signature (la vitesse de déplacement du stylo, les accélérations, la pression exercée, l'inclinaison…).
   - la façon d'utiliser un clavier d'ordinateur (la pression exercée, la vitesse de frappe…).

2. Les techniques d'analyse de la morphologie humaine
   - les empreintes digitales;
   - la forme de la main;
   - les traits du visage;
   - le dessin du réseau veineux de l'œil (l'iris et la rétine)
   - la voix

L'application de cette méthode se déroule en deux étapes séparées dans le temps :

1- Un fichier «signature» contenant un enregistrement des caractéristiques de la personne est créé.

2- La vérification de l'identité de la personne en comparant son fichier «signature» avec l'information transmise lors de l'identification.

Pour décider d'accepter la similitude entre deux «*signatures*», il faut établir un seuil d'acceptation compte tenu du niveau de sécurité souhaité.

La technologie de l'identification par la biométrie présente des avantages et des inconvénients.

Avantages

- un niveau élevé de fiabilité;
- un haut niveau de sécurité (la biométrie permet de respecter les règles de base de la sécurité comme ne pas inscrire son mot de passe à côté de l'ordinateur, désactiver l'écran de veille pour éviter des saisies de mots de passe fréquentes)
- évite les pertes de mots de passe (en effet, on ne peut pas perdre nos caractéristiques physiques comme il peut arriver avec un mot de passe. Cela évite aux administrateurs de réseaux de répondre aux nombreux appels des usagers pour perte de mot de passe, que l'on donne parfois au téléphone, donc sans sécurité)
- confort et efficacité pour l'individu (on épargne à l'individu de mémoriser des mots de passe ou de se procurer une carte d'accès)
- plus de confiance de la part des consommateurs (un moyen d'authentification connu, comme les empreintes digitales, pourrait faire changer le comportement des consommateurs qui, à l'heure actuelle, se méfient des transactions sur Internet).

Inconvénients

- des coûts élevés (En effet, la biométrie nécessite l'installation de matériel coûteux comme des caméras, des lecteurs optiques, etc.)
- manque d'uniformité et dangers d'incompatibilité (il existe plusieurs programmes et interfaces permettant l'identification biométrique qui ne sont pas toujours compatibles les uns avec les autres)

- crainte d'une surveillance gouvernementale ou policière (l'usager potentiel peut associer «empreintes digitales» à police ou à fichage)
- peu de fiabilité pour l'identification basée sur les comportements susceptibles d'être affectés par le stress
- problème de sécurité (l'interception des données est possible comme pour toutes les transactions faites sur Internet)
- de possibles impacts «biologiques» (comme dans le cas de l'identification à l'aide de l'iris)
- certaines limitations légales quant au consentement (une procédure comme l'analyse de l'iris peut entraver l'espace physique privé d'une personne et dans ce cas un consentement clair et express doit être donné)
- ces méthodes peuvent être utilisées à l'insu de la personne concernée : bouton de clavier analysant les empreintes, caméras d'analyse du visage, reconnaissance de la voix…

4.5 L'identification par le recours à un tiers

L'identification est plus sûre lorsqu'elle est attestée par un tiers qui vient affirmer que la personne qui se présente à une transaction est bien celle qu'elle prétend être.

4.5.1 La certification par un tiers

Le système de certification par les tiers vise à renforcer la fiabilité et la sécurité des mécanismes de signature basés sur la cryptographie à clé publique[49].

L'UIT-T définit la notion d'autorité de certification comme étant une *«autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat»*[50]. La notion d'autorité de certification ne se comprend que dans le cadre d'une architecture à clé publique ou, autrement dit, de signature numérique. Dans une telle architecture, l'utilisation de la clé publique permet de vérifier une signature numérique réalisée à l'aide de la clé privée correspondante. Néanmoins, il importe de s'assurer que ces clés correspondent bel et bien à l'identité avérée du signataire. Il est en effet possible d'imaginer qu'une personne utilise une paire de clés asymétriques en présentant frauduleusement celles-ci comme correspondant à l'identité d'un tiers ou d'une personne fictive. L'utilisation de certificats, émis par une autorité de certification, permet de pallier cette difficulté.

Les autorités de certification sont des entités publiques ou privées. Lorsqu'elles sont privées, elles sont généralement autorisées par les pouvoirs publics à proposer de tels

49 Pour plus d'information consulter : SYMPATICO AIDE, «Qu'est-ce qu'une autorité de certification?», http://www2.nb.sympatico.ca/Aidez/Recommandations/certauto.html, SYMPATICO AIDE, «Qu'est-ce qu'un certificat numérique?», http://www2.nb.sympatico.ca/Aidez/Recommandations/certificat_numerique.html, Strategis Canada, «Sécurité et cryptographie», http://strategis.ic.gc.ca/virtual_hosts/e-com/francais/crypto/631d13.html, Secrétariat de l'autoroute de l'information, *L'identification des citoyens et l'inforoute*, Québec, mars 1997, http://www.autoroute.gouv.qc.ca/publica/pdf/cartmicr.pdf, p. 30 et p. 35 et aussi le Glossaire à http://www.autoroute.gouv.qc.ca/publica/gloss.html, Verisign (site français) http://www.rapidsite.fr/ssl/verisign.htm et site anglais http://www.verisign.com, BelSign, http://www.belsign.be, voir aussi les résultats de recherche Yahoo! http://ink.yahoo.com/bin/query?p=autorit%E9+de+certification&hc=0&hs=0

50 UIT-T, Recommandation X.509, Annuaire - Cadre d'authentification, Fasc. VIII.8, 1988, art. 3.3 *c)*.

services, et peuvent être constituées en vertu d'une législation en la matière. Dans tous ces cas, ces entités privées peuvent être appelées à exercer leur fonction en concurrence et sous la gouverne d'une ou plusieurs autorités de certification hiérarchiquement supérieures.

Le premier rôle d'une autorité de certification consiste à émettre des certificats d'identification. De façon subsidiaire, celle-ci peut également accomplir des fonctions d'archivage, de création et de conservation de clés asymétriques.

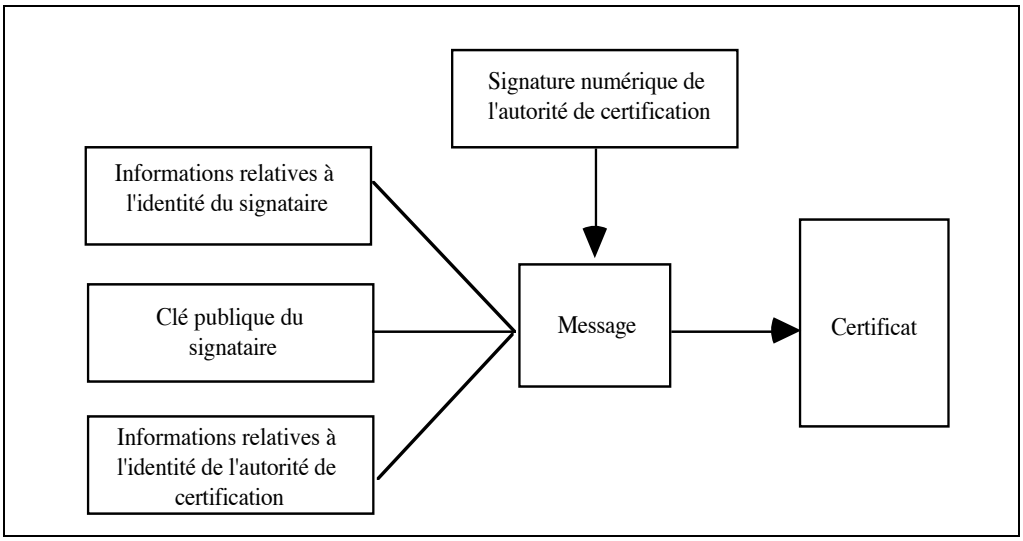
4.5.2 Les certificats

Lorsqu'il y a certification d'identité, un «tiers de confiance» (autorité de certification) émet un certificat numérique établissant l'identité de la personne ou de l'entité à qui a été attribuée une clé publique.

Un certificat est un document électronique dont l'objet est d'établir un lien entre une personne et une paire de clés asymétriques. Le certificat contient ainsi différentes informations relatives à l'identité d'un signataire, dont principalement la clé publique de celui-ci. Il est réalisé et signé par l'autorité de certification à l'aide de la cryptographie asymétrique et est, par le fait même, protégé contre les altérations. Il peut être émis, à demande, à tout signataire enregistré auprès d'une autorité de certification. L'exemple suivant illustre l'utilisation possible de certificats.

Alice transmet à Bob un message ainsi que sa signature réalisée à l'aide de sa clé privée. Elle lui transmet également un certificat numériquement signé par une autorité de certification. Après avoir reçu ces documents, Bob vérifie d'abord le certificat à l'aide de la clé publique de l'autorité de certification. Si la vérification est concluante, il est assuré de l'intégrité des informations contenues dans le certificat, soit l'identité d'Alice et de sa clé publique. Il peut ensuite utiliser la clé publique d'Alice ainsi obtenue pour vérifier la signature du message transmis par celle-ci.

Figure



Puisque les informations contenues dans un certificat sont inaltérables, celui-ci peut également être publié dans un répertoire accessible à tous les utilisateurs. Dans ce scénario, Alice n'a pas à accompagner son message d'un certificat. Pour vérifier le lien entre Alice et sa clé publique, Bob n'a qu'à consulter le répertoire de certificat. Ce répertoire atteste par ailleurs que le certificat est toujours en vigueur et n'a pas été révoqué ou suspendu.

Les certificats sont généralement valides pour une période de deux ans suivant leur émission. Ils peuvent être suspendus ou révoqués pour différentes raisons, dont le décès du signataire, la modification de la raison sociale d'une entreprise, la fin des activités d'une entreprise, la divulgation non autorisée de la clé privée, ou plus simplement à la demande du signataire. De plus, ils peuvent généralement être suspendus ou révoqués par l'autorité de certification, sans l'autorisation du signataire, lorsqu'il est raisonnable pour celle-ci de croire que la sécurité de la clé privée est compromise ou que les informations contenues dans le certificat sont erronées[51].

Aux termes de la recommandation X.509 de l'UIT-T, un certificat doit contenir : *«[la] clé publique d'un utilisateur ainsi que certaines autres informations rendues infalsifiables...»*[52]. Selon le projet FAST[53], ces «autres informations» comprennent le nom sous lequel le signataire est généralement reconnu; le nom distinctif du signataire; le numéro de série unique au certificat; la date et l'heure d'expiration du certificat.

De manière plus générale le certificat électronique établit qui est le propriétaire d'un site web ou l'identité d'une société qui transige sur Internet.

Un certificat comporte des informations comme :

- l'identité de l'autorité de certification,
- l'identité du serveur où se trouve le site Web
- la date d'expiration
- des renseignements sur le type de chiffrement qui sera utilisé pour toute transaction avec ce site.

La fiabilité du certificat dépend essentiellement de la manière dont l'autorité de certification procède à des vérifications d'identité avant son émission. Par conséquent, le degré de fiabilité d'un certificat est fonction de la qualité des mécanismes d'attribution d'identité électroniques exposés au chapitre suivant.

---

51 Voir Serge PARISIEN et Pierre TRUDEL, avec la collaboration de V. WATTIEZ-LAROSE, *L'identification et la certification dans le commerce électronique*, Cowansville, Ed. Yvon Blais, 1996.

52 UIT-T, Recommandation X.509, Annuaire - Cadre d'authentification, Fasc. VIII.8, 1988, art. 3.3 *b)*.

53 COMMISSION EUROPÉENNE, *First Attempt to Secure Trade* (FAST), TEDIS (DG III), section D, pp. 1 et 8.

4.6 Les autres techniques d'identification sur Internet

Beaucoup de mécanismes techniques sont mis en place afin de rendre la navigation sur l'Internet plus facile. Ces mécanismes n'ont pas comme objectif premier l'identification des utilisateurs. Toutefois, certains de ces mécanismes peuvent permettre de confirmer ou de déduire l'identité d'un utilisateur. Lorsqu'ils sont utilisés d'une façon détournée, ils peuvent donner lieu à des pratiques de surveillances inacceptables.

Deux catégories de traitement de données personnelles doivent être distinguées, les traitements de ciblage marketing et les traitements de données navigationnelles :

1. Les traitements de ciblage de marketing sont destinés à établir le profil des visiteurs des sites qui se sont inscrits et qui ont fourni pour cela un certain nombre de données permettant de les identifier.

2. Les traitements de données navigationnelles permettent de croiser deux sources d'information :
   - les données d'identification et de profils des visiteurs telles qu'elles ont pu être collectées lors de l'enregistrement initial des utilisateurs sur le site.
   - les données générées soit à partir de logiciels d'analyse des variables d'environnement (logs) présentes sur les plates-formes serveurs, soit à l'aide des «cookies» qui vont permettre de suivre pas à pas les rubriques consultées par les utilisateurs.

Après avoir décrit brièvement chacun des mécanismes, nous indiquerons les diverses préoccupations soulevées par ces mécanismes.

4.6.1 Les fichiers témoin (*cookies*)

Le fichier témoin, mieux connu sous le terme anglais *cookie*, est un élément d'information transmis par le serveur au navigateur lorsque l'internaute visite un site web. Le cookie est enregistré dans un fichier situé sur l'ordinateur de l'usager. Cet enregistrement peut être récupéré par le serveur lors de visites subséquentes de l'usager sur le même site. Au départ, les témoins ont été développés dans le but d'adapter dynamiquement le contenu des sites web aux habitudes de navigation de l'internaute. Aujourd'hui, son utilisation est controversée parce que le cookie est stocké sur un ordinateur sans que son propriétaire en soit nécessairement avisé.

Les cookies servent à plusieurs fins, voici quelques exemples :

- Personnaliser l'information fournie par l'usager en fonction des caractéristiques et des préférences de l'usager. Ainsi, lorsque l'usager indique ses préférences et ses goûts particuliers à l'aide d'un formulaire par exemple, ceux-ci sont stockés dans un cookie sur son ordinateur. Lors de sa prochaine visite, le site présentera des informations qui correspondent à ces préférences.
- Garder en mémoire les transactions en ligne. Un serveur de transaction électronique insère un cookie à chaque fois que le client sélectionne un produit. Lorsque l'usager se

rendra sur la page contenant le formulaire de commande, le serveur récupérera les cookies afin d'afficher l'ensemble des produits sélectionnés par le client.

- Déceler les goûts et les habitudes des usagers. Un moteur de recherche positionne des cookies en fonction des rubriques visitées par l'usager (ex. : informatique, éducation, jeux) afin, ultérieurement, d'afficher dynamiquement des bandeaux publicitaires correspondant aux intérêts ainsi décelés.

Plusieurs devoirs et obligations découlent de l'emploi des cookies par un site web[54] :

- Il faut informer le visiteur d'un site web des finalités visées par l'utilisation des cookies. Le visiteur doit être informé des finalités de la collecte et des traitements de données relatifs aux cookies au moment où ceux-ci sont placés dans le fichier correspondant de son ordinateur.
- La durée de conservation des cookies doit être déterminée et ne devrait pas être excessive.
- Il faut éviter l'implantation de cookies en rafale, qui provoque l'effet de saturation chez le visiteur du site web.
- Il faut cesser d'envoyer des cookies lorsqu'un visiteur a refusé une première fois leur implantation.
- Il ne devrait exister aucun lien de condition entre le fait de refuser l'implantation des cookies et la possibilité de naviguer librement à travers les pages web du site qui s'adressent au public.
- On doit distinguer les cookies implantés par le site même, de ceux implantés par les tiers comme les agences de publicité.
- Les usagers qui acceptent les cookies doivent être informés de la façon dont les données d'identification peuvent être rapprochées avec les informations reçues des cookies.

4.6.2 Les variables d'environnement

Lorsqu'une personne navigue sur Internet, elle établit constamment des connexions avec les différents sites qu'elle visite. Afin d'établir une connexion, chacune des requêtes comporte un certain nombre d'informations sur ce que la personne veut demander comme, par exemple, l'accès à la page web. Les requêtes contiennent également des informations sur l'environnement de l'ordinateur de la personne requérante. Ces informations sont alors transmises au serveur sous forme de variables d'environnement afin qu'il puisse exécuter la requête demandée. Ainsi, il est possible pour le serveur d'identifier les variables suivantes :

- l'adresse IP de l'usager;
- son nom de domaine (lequel révèle son fournisseur d'accès);
- son système d'exploitation;
- le type et la version du navigateur utilisé;

---

54 Source : OCDE, *Pratiques relatives à la mise en oeuvre sur les réseaux mondiaux des Lignes directrices de l'OCDE sur la vie privée*, Comité de la Politique de l'information, de l'informatique et des communications, DSTI/ICCP/REG(98)6/FINAL.

- la dernière page web visitée.

Les variables d'environnement sont des outils standards mis à la disposition du programmeur pour faciliter la programmation. Ainsi, en plaçant des informations dans de tels outils, il devient possible de les manipuler aisément. Ces informations sont transmises au serveur web pour permettre de prendre compte des éléments propres à la configuration de l'ordinateur de la personne. En accédant à ces informations, le serveur peut décider de ne pas lancer certaines applications qu'il sait incompatibles avec cet ordinateur-client.

L'identification par le serveur des composantes de l'ordinateur d'un visiteur est essentielle au bon fonctionnement de la communication dans des réseaux ouverts. Cependant, les variables d'environnement peuvent être associées à d'autres moyens d'identification comme les données nominatives transmises volontairement par l'usager, les cookies ou les fichiers d'audit. Cette association pose plusieurs problèmes à l'égard de la vie privée de l'usager :

- toute l'activité de l'usager sur le réseau Internet peut être surveillée;
- des renseignements personnels sont collectés à l'insu de l'usager;
- l'utilisateur est identifié contre son gré et à son insu;
- il est impossible de savoir quelle sera l'utilisation de ces données (elles pourront être divulguées à des tiers à des fins de marketing ou de publicité);
- ce mécanisme d'identification à partir des variables d'environnement est peu connu par la population, qui demeure sous l'impression que la navigation est anonyme.

4.6.3 Le fichier d'audit du serveur

Pour accéder à un site web, le navigateur de l'usager envoie une requête au serveur lui indiquant l'adresse Internet qu'il veut visiter. Le serveur enregistre l'ensemble de ces requêtes dans un fichier appelé « fichier d'audit ».

En analysant le fichier d'audit du serveur, il est possible d'identifier les dernières pages consultées par l'usager. Pour ce faire, il s'agit d'extraire du fichier d'audit les informations correspondant à l'adresse IP de l'usager. En effet, lorsque l'usager clique sur un lien sur la page web d'un site, son logiciel envoie au serveur qui héberge cette page un message qui lui indique l'adresse désirée. Or, pour que le serveur puisse envoyer le résultat de cette requête, il faut préalablement qu'il connaisse l'adresse de l'usager. À chacune des requêtes, le navigateur de l'usager lance une requête au serveur, récupère l'adresse IP du serveur auquel la page est demandée et contacte ce serveur. L'administrateur peut ainsi collecter les requêtes reçues sur un serveur.

L'audit doit permettre à l'administrateur de connaître la répartition des charges de son système. Ainsi, il est plus en mesure de faire les ajustements nécessaires à l'administration de son site web. Toutefois, l'analyse du fichier d'audit combinée à l'apposition de cookies et l'identification des variables d'environnement de l'ordinateur de l'usager peut fournir un profil précis de l'internaute qui permet de l'identifier de façon non-équivoque. On perçoit donc aisément la nécessité d'encadrer l'exploitation du fichier d'audit.

Le fait que le fichier d'audit est créé à l'insu de l'usager et la possibilité d'associer les informations qui y sont contenues avec d'autres moyens d'identification soulèvent plusieurs préoccupations :

- l'administrateur peut enregistrer et observer le contenu des requêtes des usagers sur son serveur. (Il devient ainsi possible de mesurer l'audience d'un site ou de produire des statistiques et connaître des informations relatives au comportement de l'usager)
- le traçage et le traitement du fichier peuvent se faire à l'insu de l'usager
- il est impossible de savoir quelle sera l'utilisation du fichier (ce fichier pourra être divulgué à des tiers à des fins de marketing ou publicité)
- ces informations rapprochées avec d'autres informations données de manière volontaire peuvent conduire à la fabrication d'un profil précis.

4.6.4 La mémoire cache

Les adresses web visitées par le navigateur de l'usager sont stockées dans un fichier cache pour une utilisation future. Lors d'une navigation subséquente, la mémoire cache accélère le parcours de l'usager. Par ailleurs, il est possible à partir des fichiers cache de savoir le parcours effectué sur le réseau par l'usager. Les fichiers cache peuvent être stockés sur l'ordinateur de l'usager ou sur un proxy.

Sur l'ordinateur de l'usager

L'ordinateur de l'usager enregistre dans un répertoire cache les pages web consultées. Ainsi, lorsque l'usager lance une requête, le navigateur commence par aller voir sur le répertoire du disque dur si la page web n'aurait pas été chargée auparavant. Si la même requête est lancée, le résultat sera plus rapide compte tenu de l'enregistrement sur le disque.

Cela soulève des préoccupations telles que celles-ci :

- un tiers peut prendre connaissance du parcours de l'usager en consultant le fichier cache;
- le fichier cache peut être copié par un tiers et divulgué à d'autres à des fins de marketing ou publicité
- les fichiers cache sont créés à l'insu de l'usager.

Sur un proxy

Le serveur proxy est généralement situé chez le fournisseur d'accès ou l'entreprise de l'usager. Il a pour fonction de vérifier, lorsqu'une requête est exécutée par un usager, si la même requête a déjà été faite précédemment. Si ce n'est pas le cas, il la lance pour l'usager et transmet le résultat qui se traduit par la page web demandée après l'avoir enregistrée sur son disque dur. Ainsi, si un autre usager du même fournisseur d'accès ou de l'entreprise lance la même requête peu de temps après, c'est le serveur de proxy qui répondra en allant la chercher simplement sur son disque dur.

Parmi les préoccupations que le procédé soulève, signalons celles-ci :

- il est toujours possible de conserver la trace des requêtes effectuées par les clients ou les employés du fournisseur d'accès;
- les fichiers cache sont créés à l'insu de l'usager
- l'usager n'a aucun contrôle sur l'utilisation de ces fichiers (divulgation aux tiers possible)
- danger de rapprochement des éléments contenus par les fichiers cache avec d'autres moyens d'identification.

4.7 Les moyens indirects d'identification

Il existe sur Internet d'autres moyens qui permettent de repérer ou obtenir des renseignements sur un individu ou une compagnie. Ces mécanismes ne permettent pas d'identifier une personne ou une compagnie lors d'une transaction. Par ailleurs, on peut grâce à eux vérifier l'identité d'une personne en confrontant les renseignements fournis par celle-ci et les informations collectées à l'aide de ces services. Voici quelques-uns de ces services.

Les listes de discussion

Les moteurs de recherche des listes de discussion permettent de dépister les messages qu'un usager a envoyés à partir de son adresse électronique. Ensuite, il est possible, après avoir lu un message, de récupérer toutes les autres interventions faites par l'usager.

Par ailleurs, les listes de discussion permettent d'avoir accès au profil de l'usager à partir de son surnom. Ce profil est toutefois établi sur la base de renseignements volontaires donnés par l'usager lors de son inscription à la liste.

Certains sites web ont comme fonction principale de fournir les outils nécessaires à la recherche et l'identification d'une personne qu'elle soit physique ou morale. Voici quatre exemples de sites présentant cette particularité :

ICQ (I Seek You)

Il s'agit d'un outil de recherche qui permet d'informer l'usager, en temps réel, que certaines personnes sont branchées. Une fois inscrit, l'utilisateur d'ICQ est invité à donner des informations le concernant afin de permettre aux autres utilisateurs de le reconnaître. L'utilisateur a aussi la possibilité d'établir une liste de personnes que le moteur de recherche utilisera pour les retrouver. Par la suite, à toutes les fois que l'utilisateur se connecte sur l'Internet, ICQ annonce sa présence et active son moteur de recherche afin de retrouver les personnes qu'il a inscrites sur sa liste. L'utilisateur est averti lorsqu'une des personnes utilise l'Internet et s'ils le désirent, la communication peut s'établir entre eux.

Canada 411

Le service offert par l'intermédiaire du site Canada 411 est l'équivalent de l'assistance annuaire téléphonique. Le site comporte plus de 10 millions d'entrées qui permettent de retracer l'adresse, le numéro de téléphone et le code postal d'une personne. Le processus est

simple, il s'agit d'inscrire le nom d'une personne qui peut être accompagné de renseignements supplémentaires comme la ville ou la province de résidence. Plus les renseignements sont complets, plus le moteur de recherche est précis.[55]

La gratuité de ce site fait en sorte que l'accessibilité aux données d'identification des personnes est devenue très simple. De plus, il est important de souligner que ce site ne contient aucune politique relative à la protection de la vie privée des personnes. D'ailleurs, la page principale de Bell Canada (www.bell.ca) possède une clause d'exonération de responsabilité à l'égard du contenu de ses sites.

Corporate Information

Il s'agit d'un moteur de recherche qui permet de trouver de l'information sur une compagnie qui possède un site web. La procédure consiste à inscrire le nom de la compagnie recherchée dans l'espace dédié à cette fin et le moteur lancera la recherche. pour enfin faire apparaître le nom de la compagnie et son profil (http://www.corporateinformation.com).

Wright Investors' Service

Ce service détaille le profil de plus de 18 000 compagnies à travers le monde. Ce profil inclut un résumé des activités de la compagnie, ses coordonnées complètes et des données sur sa situation financière (http://www.wisi.com/index.html).

	Récapitulation des préoccupations et obligations relativement à certains mécanismes d'identification
Messages électroniques	- Le site a une obligation d'avertir l'individu que le message transmis révèle son adresse électronique - Le site devra informer si une collecte d'adresse électronique est faite.
Formulaires	Plusieurs obligations incombent au site : - Les informations facultatives doivent être clairement séparées des informations obligatoires et regroupées dans un bloc distinct - Le site doit avoir une politique explicite et accessible à l'égard des données sensibles collectées. Ainsi, il doit s'engager à respecter le plus haut degré de confidentialité et de sécurité - Le site doit offrir aux usagers la possibilité de s'opposer à la collecte des informations personnelles.
Cookies	- Informer le visiteur des finalités de la collecte et des traitements de données relatifs au cookies au moment où ceux-ci sont placés dans le fichier correspondant de son ordinateur - La durée de conservation des cookies doit être déterminée et non excessive

55 Il existe bien d'autres sites qui permettent de trouver des personnes comme Yahoo People Search (www.yahooo.com/search/people/phone.html); Anywho (www.anywho.com); White pages (www.555-1212.com). Certains sites offrent aussi des moteurs de recherche qui permettent de trouver un endroit à partir d'une destination donnée. Par exemple, voir Mapblast (www.mapblast.com); CyberRouter (www.delorme.com/cybermaps/cyberrouter). Ainsi, il est possible pour un individu qui possède le numéro de téléphone d'une personne, de trouver son adresse complète à l'aide des moteurs de recherche. Ensuite, s'il ne connaît pas l'endroit, il peut utiliser le moteur qui génère la carte du lieu où est située l'adresse et se rendre à l'endroit désigné.

	- Éviter l'implantation de cookies en rafale qui provoque l'effet de saturation chez le visiteur - Cesser d'envoyer des cookies lorsqu'un visiteur a refusé une première fois leur implantation. - Il ne devrait exister aucun lien de condition entre le fait de refuser l'implantation des cookies et la possibilité de naviguer librement à travers les pages web du site qui s'adressent au public. - Informer le visiteur des finalités qu'on vise par l'emploi des cookies. - Distinguer les cookies implantés par le site même de ceux implantés par les agences de publicité. - Fournir des informations sur la façon dont les données d'identification sont rapprochées avec les informations reçues des cookies.
Variables d'environnement	Les variables d'environnement peuvent être associés à d'autres moyens d'identification comme les données nominatives transmises volontairement par l'usager, les cookies ou les fichiers d'audit. Cette association suscite plusieurs problèmes quant à la vie privée de l'usager : - Possibilité de surveillance de l'activité de l'usager sur le réseau Internet; - Des renseignements personnels sont collectés à l'insu de l'usager; - L'utilisateur est identifié contre son gré et à son insu; - Il est impossible de savoir quelle sera l'utilisation de ces données (elles pourront être divulguées à des tiers à des fins de marketing ou publicité) - Ce mécanisme d'identification à partir des variables d'environnement est peu connu par la population qui reste sous l'impression d'une navigation anonyme.
Fichier d'audit	- L'administrateur peut enregistrer et observer le contenu des requêtes des usagers sur son serveur. - Le traçage et le traitement du fichier peut se faire à l'insu de l'usager - Il est impossible de savoir quelle sera l'utilisation du fichier (ce fichier pourra être divulgué à des tiers à des fins de marketing ou publicité) - Ces informations rapprochées avec d'autres informations données de manière volontaire, peuvent conduire à la fabrication d'un profil précis du visiteur.
Mémoire cache	- Un tiers peut prendre connaissance du parcours de l'usager en consultant le fichier cache; - Le fichier cache peut être copié par un tiers et divulgué à d'autres à des fins de marketing ou publicité - Les fichiers cache sont créés à l'insu de l'usager. - L'usager n'a aucun contrôle sur l'utilisation de ces fichiers (dans le cas des fichiers enregistrés sur un proxy) - Danger de rapprochement des éléments contenus par les fichiers cache avec d'autres moyens d'identification.

5. L'attribution d'une identité dans les environnements électroniques

Dans les environnements électroniques, la fiabilité effective de la plupart des mécanismes d'identification est tributaire de la qualité et de la sécurité du mécanisme initial en vertu duquel on attribue l'identité.

L'identification peut s'effectuer de plusieurs façons et diverses méthodes existent afin de procéder à l'attribution d'une identité. Plusieurs processus s'en tiennent à l'identité que la personne s'attribue elle-même mais d'autres sont fondés sur l'attribution de l'identité par une personne ou sur l'attestation de l'identité.

5.1 L'identité que la personne s'attribue elle-même

Certains processus d'attribution de l'identité électronique sont fondés sur l'identité que la personne s'attribue elle-même. On peut dans ces approches avoir recours aux renseignements personnels qu'une personne fournit en ligne ou identifier son adresse électronique.

5.1.1 L'identification de l'adresse électronique

L'identification de l'adresse électronique d'une personne constitue une pratique qui se rapproche de l'identification de la personne. L'identité obtenue avec un tel processus est que le nom de la personne correspond à l'adresse électronique mentionnée.

À titre d'exemple, VeriSign émet des certificats en ligne après vérification de l'adresse électronique de la personne requérante (http://www.verisign.com). Le processus auquel cette personne doit se conformer est simple mais en revanche présente un faible niveau de fiabilité. L'inscription de la personne en ligne suffit et la confirmation de VeriSign consiste essentiellement à vérifier si l'adresse électronique correspond au nom du requérant. Pour ce faire, l'entreprise VeriSign possède un répertoire de noms et d'adresses électroniques qui lui permet de faire une telle vérification.

5.1.2 Les renseignements personnels fournis en ligne

Il s'agit des cas où le requérant est invité à fournir en ligne des renseignements personnels. La confirmation de l'identité de celui-ci est basée sur des critères déterminés. Ainsi, si les informations transmises correspondent bien aux données répertoriées, l'identité de la personne est confirmée. À titre d'exemple, le nom et l'adresse d'une personne peuvent être comparés aux données inscrites dans un annuaire.

Il s'agit d'une méthode d'identification automatique des personnes. VeriSign propose une méthode semblable en indiquant toutefois que l'identification de la personne n'est pas aussi certaine que lorsque le processus requiert la présence physique de l'individu.

5.2 L'identité attribuée par une personne

Ces méthodes se caractérisent par le fait qu'une personne effectue une démarche afin de constater une corrélation entre la personne et une identité électronique.

5.2.1 La vérification effectuée auprès de tiers de confiance

Afin de procéder à l'identification d'une entreprise, une vérification systématique des coordonnées de celle-ci est effectuée dans les banques de données qui proviennent du gouvernement ou détenues par tout autre tiers de confiance.

Entrust.net effectue ce genre de vérification (http://www.entrust.com). Toutefois, dans les cas où les entreprises ne sont pas enregistrées auprès d'entités gouvernementales, Entrust.net convient de faire des efforts raisonnables pour vérifier l'identité de l'entreprise en effectuant, à titre d'exemple, un appel téléphonique à son institution financière.

5.2.2 La vérification des pièces justificatives

Afin d'établir l'identité des personnes, on peut exiger la production des justificatifs d'identité et de domicile :

Pour une demande faite par un individu :

- acte d'état civil,
- permis de conduire,
- carte d'assurance maladie
- passeport
- deux justificatifs de domicile : dernière facture d'électricité, dernière facture de téléphone, dernier avis d'imposition, dernier bulletin de salaire etc.

Pour les demandes de certificats d'entreprise

- un mandat signé par un représentant de l'entreprise désignant la personne physique à qui le certificat doit être délivré. Ce mandat doit être signé pour acceptation par la personne physique bénéficiaire
- un exemplaire des statuts de l'entreprise portant signature de ses représentants
- deux justificatifs d'identité de la personne physique mandatée

L'autorité d'enregistrement établit l'identité du requérant à l'aide des pièces contenues au dossier.

5.2.3 La vérification d'identité par la présence physique des personnes

Ce processus de vérification de l'identité exige notamment la présence physique de la personne afin qu'elle présente des pièces justificatives pour établir son identité.

VeriSign et Entrust.net utilisent ce genre de procédé qui est d'ailleurs considéré comme étant l'un des plus fiables. En effet, la personne est appelée à jouer un rôle actif dans la démonstration de son identité puisqu'elle est obligée de se déplacer pour fournir les documents au soutien de ses prétentions. Les documents exigés sont, par ailleurs,

considérés comme représentant un degré élevé de fiabilité puisqu'ils émanent d'une autorité publique.

5.3 L'identité attestée

Il s'agit ici d'un processus par lequel une personne atteste que celui qui présente l'identité électronique est bien celle qu'elle prétend être.

L'identification des notaires s'exerce par l'intermédiaire de Notarius qui a mis sur pied une infrastructure à clés publiques (ICP) pour la profession notariale du Québec (http://www.icp.notarius.com).

L'infrastructure repose sur des mécanismes de sécurité permettant de s'assurer d'un niveau de sécurité équivalent, sinon supérieur, aux processus proposés précédemment.

L'autorité de certification de l'ICP de la profession notariale est la Chambre des notaires du Québec. Pour mener à bien cette tâche d'identification, la Chambre des notaires a recours à deux entités distinctes :

1. L'autorité de certification locale (ACL) qui a pour mandat de vérifier l'identité des détenteurs de signature numérique. Le secrétaire adjoint agit à titre d'autorité de certification locale lors de l'émission d'une signature numérique aux notaires. Il vérifie la conformité de la signature du notaire avec celle inscrite à l'Ordre et examine le dossier disciplinaire. En cas de non-conformité de la signature, le notaire doit se présenter en personne pour effectuer un dépôt de sa signature.

2. Le centre de certification géré par Notarius a pour mandat d'émettre les certificats d'identité.

Afin d'activer sa signature numérique, le notaire devra utiliser conjointement et simultanément deux codes d'activation transmis par deux moyens différents. Ainsi, un premier code d'activation est envoyé par huissier qui a l'obligation de le remettre au notaire en personne et d'exiger une preuve de son identité. Le huissier devra alors dresser un procès-verbal à cet effet. Le deuxième code d'activation sera transmis par l'intermédiaire du courrier électronique à l'adresse électronique personnelle du notaire.

À l'aide des codes d'activation reçus, le notaire pourra activer sa signature numérique et choisir un mot de passe qui lui permettra de signer, en tout temps, les documents électroniques qu'il désire transmettre.

La complexité et la rigueur du processus lui confère un degré de fiabilité très élevé. En effet, au moment de l'activation de la signature numérique à l'aide des codes distribués, l'identité du notaire est bien établie et il existe très peu de probabilité qu'il s'agisse d'une autre personne.

Depuis le mois d'août 1999, le Registre des droits personnels et réels mobiliers (RDPRM) permet la transmission électronique des réquisitions d'inscription. Pour ce faire, les

personnes désireuses de se procurer une signature numérique afin de transmettre leurs demandes d'inscription par voie électronique, doivent au préalable obtenir une signature numérique délivrée par l'officier du RDPRM, à la suite d'une vérification de son identité par le notaire accrédité.

La vérification de l'identité requiert la présence de la personne dont l'identité doit être vérifiée, laquelle doit produire deux pièces d'identité reconnues par les gouvernements provincial ou fédéral. Le notaire doit également recueillir le code de vérification que la personne a choisi et qu'elle seule peut utiliser pour s'identifier auprès de l'officier. Le notaire doit ensuite attester que l'identité de la personne a été établie dans un procès verbal rédigé en minutes.

Par la suite, le notaire fera parvenir au RDPRM par courrier électronique sécurisé les données recueillies sur la personne. Les autorités du RDPRM vérifieront, à leur tour, la signature numérique du notaire pour enfin faire parvenir à la personne, par courrier personnel, le certificat qui sera émis après vérification du code de vérification.

La confirmation de l'identité d'une personne par un officier public fait en sorte d'augmenter le niveau de fiabilité lors de l'identification. Par ailleurs, l'envoi par courrier électronique sécurisé du certificat qui contient la signature numérique permet une seconde fois d'obtenir l'assurance qu'il s'agit bien de la personne identifiée auparavant par le notaire.

Moyen d'identification	Niveau de fiabilité
Selon l'adresse électronique	Faible : aucune vérification n'est faite quant à l'identité de la personne; simple vérification de la conformité entre l'adresse électronique et le nom du requérant (voir Verisign)
Selon les renseignements personnels fournis en ligne	Moyen : inscription de la personne en ligne et vérification de la conformité des données transmises sur la base de critères déterminés; la vérification de l'identité se fait uniquement en ligne et sa fiabilité dépend des informations fournies par la personne.
Recherches extérieures effectuées auprès de tiers de confiance	Moyen à élevé : moyen utilisé pour identifier une entreprise. Vérification systématique des coordonnées de celle-ci effectuée dans les banques de données gouvernementales ou détenues par tout autre tiers de confiance.
Vérification de pièces justificatives	Élevé : le requérant doit produire fournir deux pièces justificatives d'identité et deux pièces justificatives de domicile. En ce qui concerne l'entreprise, le requérant doit fournir une demande écrite signée par le chef de l'entreprise, un exemplaire des statuts de l'entreprise et une pièce portant le numéro de l'entreprise et deux justificatifs d'identité de la personne physique mandatée.
Vérification avec présence physique	Très élevé : ce processus exige la présence physique de la personne qui devra établir son identité à l'aide de pièces justificatives.
Confirmation par des personnes qui exercent le rôle d'officiers publics	Très élevé : deux entités distinctes effectuent cette tâche d'identification :

(Notarius)	Afin d'activer sa signature, le notaire devra utiliser conjointement et simultanément deux codes d'activation transmis par deux moyens différents. Premier code envoyé par huissier et second, par courrier électronique à l'adresse personnelle du notaire. À l'aide des codes d'activation reçus, le notaire pourra activer sa signature numérique.
Notaire	Très élevé : la vérification de l'identité requiert la présence de la personne dont l'identité doit être vérifiée. Celle-ci doit produire deux pièces d'identité reconnues par les gouvernements provincial et fédéral et choisir un code de vérification qu'elle utilisera pour activer son certificat qui lui sera transmis par courrier électronique.

La détermination des mécanismes et processus d'identification est une démarche qui découle de l'évaluation des risques et enjeux liés à la transaction dans laquelle s'effectue la démarche.

On doit retenir les mécanismes et processus en recherchant le degré nécessaire de certitude que commandent les enjeux et les risques de la transaction ou des transactions envisagées.

Conclusion - Récapitulatif sur la conduite à tenir en matière d'identification électronique

Une entreprise ou un organisme qui décide d'offrir ses services sur Internet doit tenir compte de plusieurs préoccupations et prendre diverses précautions à l'égard de l'identification des personnes. On peut distinguer quatre étapes à cette démarche.

Première étape : Spécifier les besoins d'identification
Dans un premier temps, on doit se demander si l'identification de l'individu est nécessaire. L'identification peut s'avérer nécessaire en tant que composante d'une transaction. Par exemple, il est nécessaire de connaître l'adresse postale d'une personne pour effectuer la livraison d'un produit. Également, la loi exige souvent d'identifier un individu, par exemple, la loi sur le tabac interdit la vente des cigarettes aux moins de 18 ans. Finalement, une obligation d'identifier existe lorsque la transaction est telle que la prudence ou la bonne gestion impose que l'on identifie une partie.

Deuxième étape : Déterminer le degré de certitude requis pour l'identification
Au cours de cette seconde étape, il faut répondre à la question « Quel est le degré de certitude requis pour l'identification? ».

Compte tenu des enjeux et des risques des transactions qui seront réalisées dans l'environnement considéré, il s'agit ici de spécifier le degré de certitude dont on a besoin en matière d'identification. Par exemple, plus la transaction est importante, plus le niveau de fiabilité exigé sera élevé.

Troisième étape : Baliser la collecte et le traitement de l'information personnelle
Lorsque l'identification est nécessaire et après avoir déterminé le degré de certitude qui est requis, il faut considérer les limites imposées au nom de la protection de la vie privée des personnes. La loi empêche une entreprise ou un organisme d'exiger des renseignements personnels sur un individu qui ne sont pas nécessaires à la conclusion de la transaction ou à son exécution. Ainsi, selon la nature de la transaction ou des services à offrir, il faut limiter la collecte d'informations à celles qui sont strictement nécessaires pour la réalisation de cette transaction.

Quatrième étape : Déterminer les mécanismes et processus d'identification
Le choix de techniques et de mécanismes d'identification intervient en quatrième étape. Ces mécanismes et processus d'identification devront permettre d'identifier la personne avec un minimum d'informations personnelles et selon un niveau de fiabilité acceptable en conformité avec l'importance de la transaction.

Une fois l'identification effectuée, la loi impose plusieurs obligations quant à la collecte et le traitement des renseignements personnels. L'entreprise ou l'organisme doit informer l'individu du but de la collecte, de l'utilisation qui sera faite des renseignements, des catégories de personnes pouvant consulter son dossier, de l'endroit où il est détenu ainsi que de ses droits d'accès et de rectification à son dossier. De la même manière, l'entreprise qui détient, utilise ou communique les renseignements personnels ainsi obtenus doit en

assurer la confidentialité. Elle doit voir à leur exactitude et à leur mise à jour au moment de les utiliser. Elle doit obtenir le consentement de l'usager lorsqu'elle désire les communiquer ou les utiliser à d'autres fins que celles déjà établies.

Annexe 1
Tableaux

Tableau 1
Exemples de l'obligation de s'identifier en vertu de la loi

	Loi	Obligation
Vérification d'âge pour la consommation de certains produits ou la présence dans certains endroits	*Loi sur les infractions en matière de boissons alcooliques*, L.R.Q., c. I-8.1, art. 103.5	*Toute personne peut être requise de prouver qu'elle est majeure* lorsqu'elle désire acheter des boissons alcooliques, être admise dans une brasserie, une taverne ou un bar [...] ou demeurer, après vingt heures, sur une terrasse de l'un de ces établissements.
	Loi sur le Tabac, L.C. (1997) c. 13, art. 8(1)	(1) il est interdit, dans les lieux où le public a normalement accès, de fournir des produits du tabac à un jeune (2) Une personne ne peut être reconnue coupable d'une infraction au paragraphe (1) *s'il est établi qu'elle a tenté de vérifier si la personne avait au moins dix-huit ans* en demandant et examinant une pièce d'identité conforme aux règlements et qu'elle avait des motifs raisonnables de croire que la pièce était authentique.
	Règles sur les appareils de loterie vidéo, (1984) 116 G.O.II 4908, art. 46	Le titulaire d'une licence d'exploitant de site, la personne responsable [...] ou un membre du personnel de l'établissement *ne peut effectuer le paiement d'un coupon sans avoir vérifié au moyen d'un passeport, d'une copie d'un acte de naissance, d'un permis de conduire d'un véhicule automobile ou d'une carte d'identité*, que la personne qui réclame le paiement d'un coupon de remboursement est majeure ou si elle l'est, qu'elle ne réclame pas ce paiement pour le compte d'une personne mineure.
Pouvoir des agents de la paix d'identifier une personne	*Code de procédure pénale*, L.R.Q. c. C-25.1, art. 72 et 74	L'agent de la paix qui a des motifs raisonnables de croire qu'une personne a commis une infraction peut exiger qu'elle lui déclare ses nom et adresse, s'il ne les connaît pas afin que soit dressé un constat d'infraction
Identification criminelle	*Loi sur l'identification des criminels*,L.R.(1985), c. I-1, art. 2	Les personnes déclarées coupables d'un acte criminel sont obligées à coopérer à certains actes d'identification (tels la «prise d'empreintes digitales, des photographies et de toute autre mensuration ainsi que tout autre opération anthropométrique.»)

Tableau 2
Exemples d'identification sans le soutien de document

Texte de loi	Informations requises
Loi sur les accidents du travail et maladies professionnelles, L.R.Q. c. A-3.001, art. 268 (procédure de réclamation)	- nom et prénom - adresse de l'employé - numéro d'assurance sociale et - numéro d'assurance maladie.
Règlement sur le régime général d'assurance médicaments, (1996) 128 G.O.II 6734, art. 7 (Inscription au régime d'assurance-médicaments)	- nom et prénom - sexe; - date de naissance; - numéro d'assurance maladie; - numéro d'assurance sociale, le cas échéant; - adresse; - son emploi ou sa profession.
Règlement sur l'admissibilité à l'aide juridique, (1985) 115 G.O.II 2343, art. 6.(demande d'aide juridique)	- nom et prénom - l'adresse de l'individu; - numéro d'assurance sociale; - nom et adresse de l'employeur.

Tableau 3
Exemples d'identification avec le soutien de document

Lois	Informations et documents nécessaires
Règlement sur l'admissibilité et l'inscription des personnes auprès de la Régie de l'assurance-maladie (1992) 124 G.O.II, 6236; articles 14 et 15.	- nom, date de naissance, - sexe et état civil - adresse résidentielle - numéro de téléphone; - numéro d'assurance sociale (...) - une photographie couleur prise au cours des six derniers mois, datée au verso à l'aide d'un dateur - l'original de la copie de l'acte de naissance - l'original du certificat de naissance - une copie du certificat de citoyenneté canadienne - une copie des pages du passeport canadien contenant les renseignements relatifs à l'identité
Règlement sur l'assurance-emploi, (1993) 130 Gaz.Can II 2192 (attribution du numéro d'assurance sociale)	- le nom au complet - le nom à la naissance, s'il diffère de celui qu'elle porte au moment où la demande est faite; - la date de naissance et le lieu de naissance - le nom complet de la mère à la naissance - le nom complet du père à la naissance
Règlement relatif au changement de nom et d'autres qualités de l'état civil, (1993) 125 G.O.II 8053	- nom, tel qu'il est constaté dans l'acte de naissance; - sexe; - la date et le lieu de sa naissance ainsi que l'endroit où elle a été enregistrée; - l'adresse du domicile à la date de la présentation de la demande - la date à laquelle le requérant est devenu citoyen canadien, s'il est né ailleurs qu'au Canada; - les noms de ses pères et mères; - son état civil et, s'il est marié le nom de son conjoint ainsi que les dates et lieux de son mariage; - le nom de ses enfants, s'il en a, ainsi que leur date de naissance et le nom de l'autre parent de chacun d'eux. - la copie des actes de naissance, de mariage et de décès mentionnés à la demande, lorsque ces actes ont été faits hors du Québec; - copie du certificat de citoyenneté canadienne du demandeur; - copie du jugement irrévocable ou du certificat de divorce du demandeur, le cas échéant;

Tableau 4
Exemples d'identification accompagnée de formalités

Lois	Formalités supplémentaires
Loi électorale, L.R.Q., c. E-3.3, art 241.	- une lettre du chef du parti autorisé qui reconnaît la personne comme candidat de ce parti; - une photographie conforme aux normes prescrites par règlement et signée au verso par deux électeurs de la circonscription qui connaissent
Règlement sur la déclaration de candidature, (1989) 121 G.O.II 1964, art. 5	- lorsqu'une personne pose sa candidature sous ses nom et prénom usuels et que ceux-ci sont différents de ceux indiqués dans l'acte de naissance, cette personne doit joindre à sa déclaration de candidature une déclaration *sous serment* à l'effet que ses nom et prénom usuels sont de notoriété constante dans la vie politique, professionnelle ou sociale
Loi électorale du Canada, L.R.C. (1985) c. E-2, art. 81.1.	- Un bulletin de présentation doit être rédigé selon la formule prescrite contenant une déclaration, *sous serment* du candidat, énonçant : (i) les nom, adresse, occupation et appartenance politique du candidat. (ii) un serment par écrit, selon la formule prescrite, prêté devant le directeur du scrutin, par la personne qui a signé le bulletin de présentation à titre de témoin du consentement du candidat à sa présentation, déclarant qu'elle connaît le candidat

Tableau 5
Exemples d'identification attestée par un officier public

Lois	Dispositions pertinentes
Code civil du Québec, L.Q. (1991) c. 64 (articles qui concernent les inscriptions au bureau de la publicité des droits)	Art. **2988**: Le notaire qui reçoit un acte visant l'inscription ou la suppression d'un droit sur le registre foncier, ou la réduction d'une inscription, *est tenu d'attester qu'il a vérifié l'identité*, la qualité et la capacité des parties, que le document traduit la volonté exprimée par les parties et, le cas échéant, que le titre du constituant ou du dernier titulaire du droit visé est déjà valablement publié. Art. **2989**: L'arpenteur-géomètre *est tenu d'attester qu'il a vérifié l'identité*, la qualité et la capacité des parties à un procès-verbal de bornage dressé par lui, même celui fait sans formalité; le cas échéant, il est tenu d'attester que le document traduit la volonté exprimée par les parties. Art. **2990**: Les officiers de justice, les syndics de faillite, les secrétaires ou greffiers municipaux et les officiers ministériels rédacteurs d'actes authentiques ou publics. doivent *attester qu'ils ont vérifié l'identité* des personnes visées par les actes dressés par eux et soumis à la publicité foncière. Art. **2991**: L'acte sous seing privé visant l'inscription ou la suppression d'un droit sur le registre foncier, ou la réduction d'une inscription, doit indiquer la date et le lieu où il a été dressé; il y est joint *l'attestation par un notaire ou un avocat qu'il a vérifié l'identité*, la qualité ou la capacité des parties, la validité de l'acte quant à sa forme, que le document traduit la volonté exprimée par les parties et, le cas échéant, que le titre du constituant ou du dernier titulaire du droit visé est déjà valablement publié. Art. **2994**: La réquisition d'inscription sur un registre foncier de droits constatés dans un acte qui n'a pas fait l'objet d'une attestation, au moment où l'acte a été dressé, doit prendre la forme d'un sommaire. *L'identité*, la qualité et la capacité des parties au sommaire, ainsi que l'exactitude de son contenu, doivent être attestées. Art. **2995**: Aucune attestation n'est requise pour l'inscription sur le registre des droits personnels et réels mobiliers. Pour l'inscription sur le registre foncier des déclarations de résidence familiale, des baux immobiliers ou des avis prévus à la loi, à l'exception des avis requis pour l'inscription d'une hypothèque légale ou mobilière, ou de l'avis cadastral d'inscription d'un droit, les documents présentés n'ont pas à être attestés par un notaire ou un avocat, *mais par deux témoins, dont l'un sous-serment*. L'identité des parties à tout autre réquisition d'inscription sur le registre des droits personnels et réels mobiliers est tenue pour vérifiée.
Loi sur le notariat, L.R.Q, c. N-2	Art. 40 : 1. L'acte notarié est clos par la signature des parties, du notaire assistant et des témoins requis suivant le cas, *en présence du notaire instrumentant* et par la signature de ce dernier, qui doit être apposée le même jour où l'a dernière des parties à signer l'a fait. (...) Art. 41: *Le notaire doit vérifier l'identité des parties* dont il reçoit la signature par tout moyen raisonnable lui permettant d'établir cette identité. Lorsque la signature de l'une des parties est reçue par un notaire autre que le notaire instrumentant conformément au paragraphe 2 de l'article 40, il appartient *à cet autre notaire de vérifier l'identité* de la partie concernée.
Règlement sur la tenue des dossiers et des études des notaires,	Art. 21.3: Le notaire *doit conserver au dossier une preuve de vérification de l'identité* et des pouvoirs d'agir de toute partie à un acte.

Lois	Dispositions pertinentes
(1995) 127 G.O.II 1923	
Code civil du Québec, L.Q. (1991), c. 64	Art. 373: Avant de procéder au mariage, *le célébrant s'assure de l'identité*, de l'âge et de l'état matrimonial des futurs époux.

Tableau 6
Les préoccupations rattachées à l'identification des personnes

Enjeux	Exemples des préoccupations
Protection de la vie privée (protection des données personnelles)	- abus des capacités offertes par l'informatique d'accès d'enregistrement, de tri, de comparaison et d'association des caractères alphanumériques et des informations issues de la voix et de l'image - collecte de données à l'insu de l'utilisateur - création de base de données comportementales - élaboration de profils de consommation - achat ou troc de données personnelles - rapprochement des données personnelles risquant d'influencer la perception des personnes sur le passé d'un individu - demande ou collecte de données personnelles non pertinentes, compte tenu des finalités de l'organisme - utilisation des données personnelles recueillies à des fins étrangères aux finalités de leur cueillette - dispersion des données personnelles recueillies à des fins étrangères aux finalités de leur cueillette. - vulnérabilité des enfants compte tenu du fait qu'ils ne possèdent pas la capacité de donner un consentement éclairé et qu'ils sont généralement plus influençables. - crainte d'une possible surveillance gouvernementale ou policière (le *Big Brother*) - utilisation abusive des *cookies*
Protection des utilisateurs	Garanties devant être offertes aux utilisateurs - les données personnelles soient exactes, complètes et mise à jour - contrôle par l'usager de l'exactitude des données stockées sur son compte et, en cas de besoin, de les faire rectifier - l'individu doit être en mesure d'identifier le maître de fichier responsable de la collecte et du stockage des données
Sécurité des transactions	- l'authentification du message - l'identification des parties qui communiquent - l'intégrité des données personnelles - l'assurance que les transactions ont été autorisées Exemples : - l'interception des données personnelles, - l'emploi de fausses identités ((la mascarade) - appropriation non détectée, par un tiers d'un numéro permettant l'identification individuelle d'une personne (ex. : numéro de carte de crédit) - autres moyens frauduleux, - l'effacement de données personnelles - la perte de données personnelles

Annexe 2
La signature numérique

a) La signature numérique fondée sur la cryptographie asymétrique (RSA)

Les procédés de signature à clés publiques[1], ou encore de signature numérique, sont de plus en plus utilisés dans le commerce électronique et présentent, outre l'identification des parties, d'autres avantages. Ils permettent tout d'abord d'assurer l'intégrité d'un message. Autrement dit, ils garantissent que le message n'a subi aucune altération entre le moment de sa signature et de sa réception par l'autre partie. Ils permettent par ailleurs, au chapitre de la confidentialité, de garantir que seul le système informatique du destinataire est en mesure de lire le message transmis. Il s'agit là d'avantages indéniables, qui n'existent pas dans un environnement papier, et qui permettent de répondre aux plus hautes exigences en matière de sécurité.

Dans un système à clé publique, la réalisation des différentes fonctions d'identification suppose qu'une personne dispose de deux clés mathématiques complémentaires : une clé privée, dont le caractère secret doit effectivement être préservé, et une clé publique, qui peut être librement distribuée. La clé privée permet de signer le message. L'opération de décodage s'effectue, quant à elle, selon le principe de la complémentarité des clés : un message encodé avec une clé privée ne peut être décodé qu'avec sa clé publique complémentaire. L'exemple suivant illustre le fonctionnement de la signature numérique.

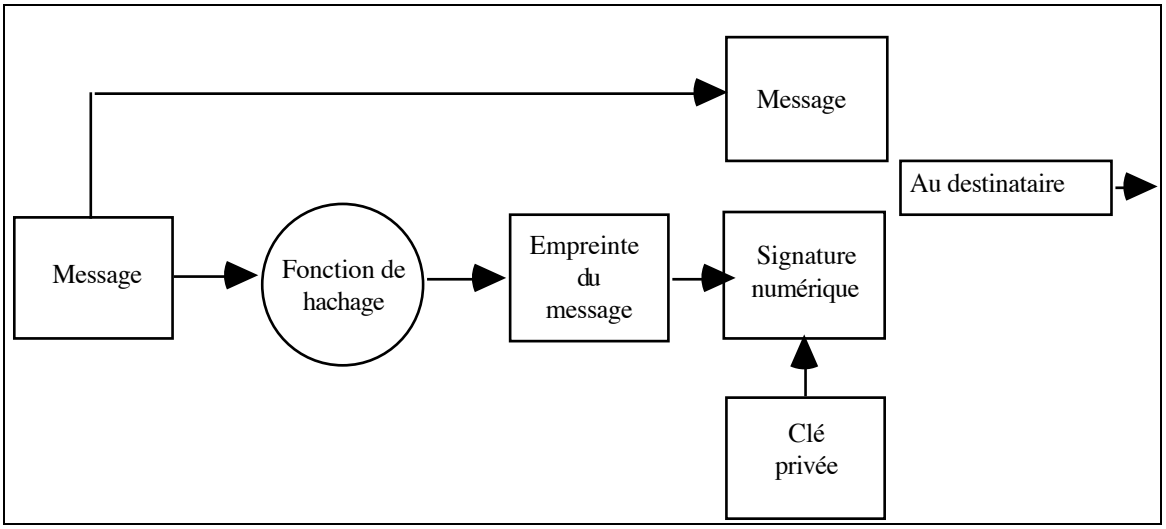
Alice désire envoyer à Bob un message informatisé signé de façon électronique. Après avoir écrit son message, Alice réalise un condensé de ce message (message digest) à l'aide d'une opération mathématique. Ce condensé digital est le résultat d'une fonction appelée fonction de hachage irréversible (*«one way hash function»* ou *«message digest function»*). Cette fonction permet de générer de façon concise une chaîne de données caractéristique du message en question. Cette représentation est sécuritaire, très concise et permet de détecter tout changement apporté au message. En effet, il suffit au destinataire d'appliquer la fonction «hachage» au message reçu et de comparer le condensé ainsi obtenu avec celui transmis par l'émetteur. Toute différence entre les condensés signifie que le message a été altéré en cours de transmission.

Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l'aide de la clé privée d'Alice. Ce condensé encodé constitue la signature numérique. Alice envoie alors à Bob son message (en clair) accompagné de la signature numérique.

---

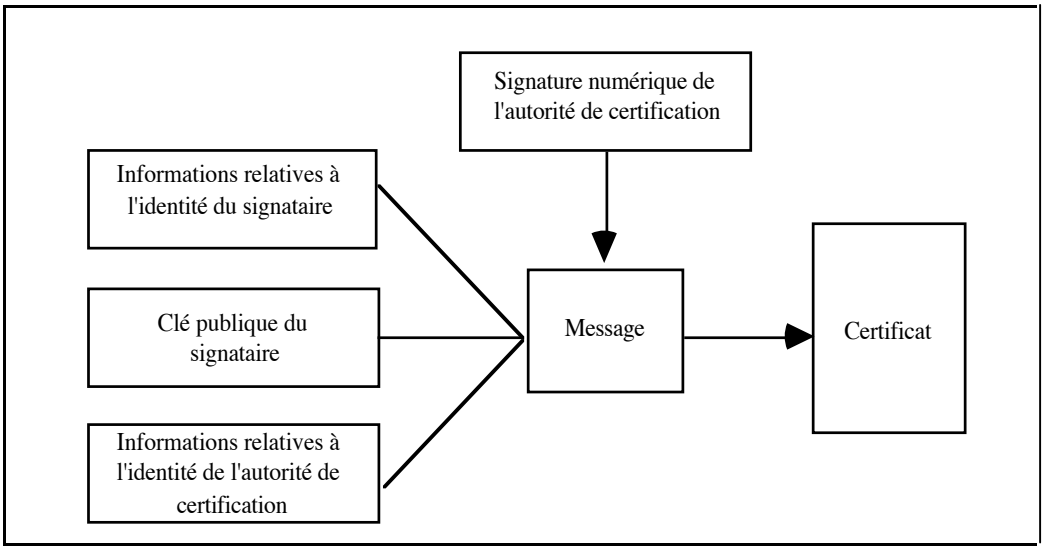
1 La cryptographie asymétrique, dite «à clé publique», a été conçue en 1975 par deux ingénieurs électroniciens, Whitfield Diffie et Martin Hellman de l'Université de Stanford, et réalisée par Ronald Rivest, Adi Shamir, et Leonard Adleman du Massachusetts Institute of Technology. Voir : PARISIEN, S. et P. TRUDEL, avec la collaboration de V. WATTIEZ-LAROSE, *L'identification et la certification dans le commerce électronique: Droit, sécurité, audit et technologies*, Cowansville, Éditions Yvon Blais, 1996; *Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM)*, juin 1994, p. 44 : ftp://ftp.cpsr.org/cpsr/privacy /crypto/acm_crypto_study.txt.

Figure I



Lorsque Bob reçoit le message et la signature, il décode la signature numérique en effectuant une opération mathématique impliquant la clé publique complémentaire d'Alice. S'il parvient à décoder la signature, Bob est assuré que celle-ci a préalablement été réalisée avec la clé privée complémentaire d'Alice : il sait alors de manière certaine qu'elle est l'auteur du message. Grâce à la fonction de hachage, il est par ailleurs assuré de l'intégrité du message d'Alice.

Figure II



La principale application de signature à clé publique (numérique) est celle proposée par la firme RSA. Sa fiabilité et son haut degré de sécurité en font un standard *de facto* en matière de commerce électronique[2]. La technologie RSA fait d'ailleurs partie intégrante de différents standards officiels à travers le monde. Il figure ainsi dans le standard 9796 de l'ISO à titre d'algorithme compatible, tout comme dans le standard X.509 de l'UIT-T (CCITT). La technologie RSA est également incorporée dans les standards de SWIFT, d'ETEBAC 5, et fait partie du projet de standard ANSI X9.31[3].

La technologie RSA était brevetée. Le brevet, détenu depuis 1983 par la firme Public Key Partners (PKP) de Sunnyvale en Californie[4], a expiré en l'an 2000.

b) Le Digital Signature Standard

Ayant débuté ses travaux en 1989, le *National Institute of Standard and Technology* (NIST) a annoncé le 19 mai 1994 l'achèvement du *Digital Signature Standard* (DSS) et son adoption à titre de *Federal Information Processing Standard* (FIPS)[5]. L'algorithme de signature spécifié dans le DSS est le *Digital Signature Algorythm* (DSA). Il peut être utilisé pour la messagerie électronique, le transfert de fonds électronique, l'EDI, l'archivage ou plus généralement pour toute application nécessitant une assurance quant à l'intégrité et à l'origine des données transmises[6]. Il est destiné à être employé à titre de standard par le secteur public et, sur une base volontaire, par tout intervenant du secteur privé[7]. Cet algorithme est mis gratuitement à la disposition du public. Il s'agit d'ailleurs de l'une des raisons invoquées par le NIST pour ne pas adopter le populaire RSA à titre de standard. Celui-ci préférait en effet sélectionner un algorithme libre de tout brevet et pouvant être utilisé sans frais par le secteur privé[8].

Tout comme pour RSA, le DSA utilise une clé privée dans le but de réaliser une signature et une clé publique complémentaire afin de la vérifier. Il est basé sur un cryptosystème proposé par ElGamal[9]. À la différence de la technologie RSA, le DSA n'est cependant pas réversible et ne peut donc être utilisé afin de chiffrer un message. C'est d'ailleurs l'une des

---

2 RSA, *RSA's FAQ About Today's Cryptography :* http://www.rsa.com/rsalabs/faq/ faq_rsa.html.

3 RSA, *RSA's FAQ About Today's Cryptography :* http://www.rsa.com/rsalabs/faq/ faq_rsa.html.

4 *U.S. Patent* 4,405,829, accordé le 9/20/83.

5 NIST, *FIPS Publication* 186, 19 mai 1994.

6 UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 septembre 1994 : http://otabbs.ota.gov/E511T93.

7 NIST, *FIPS Publication* 186, 19 mai 1994.

8 UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 septembre 1994, http://otabbs.ota.gov/E511T93.

9 US Patent 5, 231,668. Voir T. EL GAMAL, «A public-key cryptosystem and a signature scheme based on discrete logarithms», dans *IEEE Transactions on Information Theory*, vol. IT-31, 1985, pp. 469-472.

raisons pour lesquelles le processus de sélection d'un algorithme de signature a été si ardu. Le NIST, bien que voulant mettre de l'avant un algorithme de signature sécuritaire, ne voulait pas, en revanche, que celui-ci puisse également être utilisé afin de chiffrer des messages de manière à ce que les forces de l'ordre soient dans l'impossibilité de les déchiffrer[10].

Le DSA a reçu un accueil plutôt mitigé de la part du secteur privé. Plusieurs auraient en effet souhaité la sélection de RSA comme standard officiel du gouvernement américain[11]. Devant l'existence du standard *de facto* RSA, on reproche au NIST de créer, avec l'introduction du DSA, une confusion indue auprès des utilisateurs, des fabricants de logiciels et de l'industrie informatique en général. On reproche au surplus au NIST d'avoir employé, pour le choix du DSA, un processus de sélection secret et arbitraire.

Des autres critiques adressées au DSA, on peut souligner celle relative à la vérification de la signature. Bien que la réalisation de la fonction de signature soit plus rapide sous le DSA, la vérification de la signature s'effectue quant à elle de façon plus rapide sous le RSA. Il semble que cette dernière caractéristique soit plus recherchée par l'industrie que la capacité à signer rapidement un document[12].

Néanmoins la critique la plus sérieuse à l'encontre du DSA a trait à la sécurité. Contrairement au modèle d'origine proposant une clé cryptographique de 512 bits, le DSS autorise désormais l'utilisation de clés cryptographiques pouvant aller jusqu'à 1024 bits[13]. Néanmoins, de l'avis d'experts en cryptographie, la création du DSA demeure trop récente et n'a pas fait l'objet d'un nombre suffisant d'études pour que les utilisateurs puissent s'y fier[14]. Règle générale, un cryptosystème doit être disponible sur le marché durant plusieurs années avant que les inévitables erreurs de conception puissent être identifiées et adéquatement corrigées. En ce sens, quelques chercheurs ont d'ailleurs mis en garde les utilisateurs du DSA contre l'existence de «portes cachées» permettant vraisemblablement de percer les défenses de ce dernier plus aisément[15].

---

10 UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 septembre 1994, http://otabbs.ota.gov/E511T93.

11 Voir notamment : E. MESSMER, «NIST stumbles on proposal for public-key encryption. Network World», (1992) 9 *Network World* 30; NIST, «The Digital Signature Standard : Proposal and Discussion», (juillet 1992) 35 *Communications of the ACM* 36-54.

12 RSA, *Capstone, Clipper and DSS* : http://www.rsa.com/rsalabs/faq/faq_ccd.html#ccd.3.

13 UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 septembre 1994, http://otabbs.ota.gov/E511T93.

14 M.E. SMID et D.K. BRANSTAD, «Response to comments on the NIST proposed Digital Signature Standard», dans *Advances Cryptology - Crypto '92*, New York, Springer-Verlag, 1993.

15 M.E. SMID et D.K. BRANSTAD, «Response to comments on the NIST proposed Digital Signature Standard», dans *Advances Cryptology - Crypto '92*, New York, Springer-Verlag, 1993.

Annexe 3
Les techniques biométriques

a) Les empreintes digitales

Un lecteur optique prend une image de l'empreinte du doigt de l'individu. Cette image est comparée avec le fichier «signature» détenu par l'autre partie. Il est nécessaire d'avoir un lecteur pour la prise d'image des empreintes digitales, un logiciel de traitement des algorithmes pour l'extraction des minuties de comparaison et enfin une unité électronique de traitement (en général un ordinateur).

b) La main

Le système prend une photo de la main et examine quatre-vingt-dix caractéristiques, y compris la forme tridimensionnelle de la main, de la longueur et de la largeur des doigts et de la forme des articulations.

Des lumières infrarouges et un appareil photo digital sont employés pour capturer les données de la main. Aucune vérification d'empreinte digitale n'est utilisée. Un descripteur mathématique de la géométrie de main est créé à partir de ces informations et est enregistré dans le lecteur.

Pour utiliser la géométrie de la main, l'utilisateur place sa main sur une platine possédant des guides pour positionner les doigts.

Les lecteurs de la géométrie de main offrent un niveau très raisonnable d'exactitude, mais peuvent avoir des taux de fausses acceptations élevés pour des jumeaux ou d'autres membres de la même famille.

La grande taille des lecteurs de géométrie de la main peut constituer un obstacle à leur utilisation.

c) Le visage

La plupart des systèmes d'identification du visage utilisent du matériel standard, un ordinateur et une caméra pour capturer l'image.

L'image est enregistrée dans une base de données. Ces systèmes utilisent des mesures de distance entre divers éléments du visage comme moyen de vérification.

Les variables telles que des lunettes de soleil, des moustaches et des barbes, des expressions faciales anormales et l'inclinaison importante de la tête peuvent causer des dysfonctionnements avec des systèmes d'identification du visage

d) La voix

Les systèmes d'identification de la voix se concentrent sur les seules caractéristiques de la voix qui sont uniques à la configuration de la parole d'un individu. Ces configurations de la parole sont constituées par une combinaison de facteurs comportementaux et physiologiques.

La plupart des systèmes d'identification de la voix utilisent l'affichage d'un texte, des mots spécifiques doivent être lus puis parlés afin de vérifier que la personne à authentifier est bien présente et qu'il ne s'agit pas d'un enregistrement.

Les imitateurs essaient habituellement de reproduire les caractéristiques vocales qui sont les plus évidentes au système auditif humain et ne recréent pas les caractéristiques moins accessibles qu'un système automatisé d'identification de voix analyse. Il n'est donc pas possible d'imiter la voix d'une personne inscrite dans la base de données.

e) L'iris (ou la rétine)

Les deux iris d'un individu ont à peu près la même couleur mais leur forme (enchevêtrement des tubes) est aussi différente que celle de l'iris d'une autre personne. Ainsi, deux vrais jumeaux ont quatre iris autant différenciés que ceux de deux personnes aléatoirement sélectionnées. Les iris sont suffisamment variés pour qu'une approximation de l'information totale suffise à certifier l'identité d'un individu.

Dans une première étape, à l'aide d'une caméra noir et blanc et d'un capteur classique, on extrait les paramètres caractéristiques de l'iris. Dans une deuxième étape, on compare les informations collectées avec les informations sauvegardées.

f) La signature dynamique

La vérification (dynamique) de signature manuscrite est basée sur la différentiation entre les parties d'une signature qui sont habituelles et celles qui changent avec presque chaque signature.

Les systèmes d'authentification de signature incluent habituellement un crayon lecteur et une tablette à digitaliser. La vérification est accomplie en analysant un certain nombre de variables, dont la vitesse avec laquelle la signature est réalisée, les accélérations, la pression exercée, le rythme des variations du stylo et même le calcul de la distance de la plume suspendue entre deux lettres au-dessus de la tablette.